# General Terms & Conditions

## Section I - Introductory and General Terms

### Art. 1 - Introduction and Parties

**(1)** These Terms & Conditions constitute a legally binding agreement between PeopleBotApp, Inc., a Delaware corporation with principal offices at San Ramon, CA, USA ("PeopleBotApp," "Provider,"), and the individual or entity accessing or using the PeopleBotApp platform ("Customer," "you," or "your").

**(2)** The Provider operates an artificial intelligence-powered human resources assistant platform designed to support recruitment, candidate screening, and employment-related content generation. The platform functions as a co-pilot and recommendation engine, with all final employment decisions requiring human review and approval.

**(3)** These Terms & Conditions apply to all Customer access to and use of the Platform, regardless of subscription tier, payment status, or geographic location. Additional terms may apply to specific features or enterprise customers as specified in Order Forms or Master Service Agreements.

### Art. 2 - Definitions

For the purposes of these Terms & Conditions, the following capitalized terms shall have the meanings set forth below:

**"Agreement"** means the collective ensemble of these General Terms & Conditions together with the AI Transparency & Use Policy, Privacy Policy, Cookie Policy, and any specific Order Forms or Master Service Agreements incorporated by reference.

**"Platform"** means the AI-powered human resources assistant software-as-a-service (SaaS) operated by PeopleBotApp, Inc., including its interface, algorithms, tools, and all associated technical infrastructure.

**"AI Output"** means the generated text, analysis, recommendations, scores, or content (such as job descriptions and candidate summaries) produced by the Platform's AI models in response to Customer Data and inputs.

**"Customer Data"** means all proprietary information, candidate resumes, employee records, job descriptions, and any other text or media uploaded to or created within the Platform by the Customer or its Authorized Users.

**"Authorized User"** means any individual employee, consultant, or agent authorized by the Customer to access and use the Platform under the Customer's account credentials.

**"Subscription Term"** means the duration for which the Customer has purchased access to the Platform (monthly or annual), including any successive renewal periods.

**"AI Co-Pilot"** refers to the specific advisory functionality of the Platform designed to provide structured suggestions and recruitment support intended for human review, rather than automated decision-making.

**"Business Customer"** means any legal entity or individual using the Platform for purposes related to their trade, business, craft, or profession, and who is not classified as a "Consumer."

**"Consumer"** means a natural person acting wholly or mainly outside their trade, business, or profession, who benefits from mandatory statutory protection rights in specific jurisdictions (e.g., EU or India).

**"Overage Fees"** means the usage-based charges incurred by the Customer for consumption (e.g., AI queries, data storage, API calls) that exceeds the base allocation included in their selected subscription tier.

**"Service Level Agreement (SLA)"** refers to the Provider's commitment regarding Platform uptime, performance standards, and the specific remedies (such as service credits) available to Customers in the event of outages.

**"Personal Data"** means any information relating to an identified or identifiable natural person (including candidates and employees) processed through the Platform in accordance with applicable laws like GDPR or the India DPDP Act.

**Art. 3. Contractual Acceptance and Platform Scope**

**(1)** These Terms & Conditions (the "Agreement") govern the contractual relationship between **PeopleBotApp, Inc.** (the "Provider") and any individual or organization (the "Customer") that registers for, accesses, or uses the PeopleBotApp platform (the "Platform").

**(2)** By accessing the Platform, creating an account, or completing the registration process, the Customer explicitly acknowledges reading, understanding, and agreeing to be bound by these Terms & Conditions. If the Customer is entering this Agreement on behalf of a legal entity, the Customer represents they have the authority to bind that entity to these terms.

**(3)** The Platform provides an AI-powered human resources assistant for tasks like recruitment support, candidate screening, and content drafting. The AI functions strictly as a co-pilot or recommendation engine. It generates structured suggestions and analyses to inform the Customer's decisions but does not make or execute automated hiring or employment decisions on the Customer's behalf.

**Art. 4. Governing Documents and Amendments**

**(1)** This Agreement consists of these Terms & Conditions and the following documents, incorporated by reference: the AI Transparency & Use Policy (AI Policy), the Privacy Policy, the Cookie Policy. The hierarchy of documents, in descending order of precedence.

**(2)** In the event of a conflict, the document higher in the hierarchy shall prevail, **unless** the lower-tier document explicitly states its intent to supersede or modify a specific provision of the higher-tier document.

**(3)** The Provider may modify these terms. Notice of material changes will be provided at least thirty (30) days prior to the effective date via email or prominent Platform notification. Continued use of the Platform after the effective date constitutes acceptance of the modified terms.

**(4)** These Terms & Conditions are maintained under version control. The current version number and effective date are displayed at the top of the first page; When the Provider make material changes to these terms, will publish both:

1. The updated terms with changes highlighted, and
2. A summary document explaining what changed and why;

**(5)** If you continue using the Platform after the effective date of modified terms, you accept those modifications. If you do not accept material changes, you may terminate your subscription before the effective date per Art. 16

**Art. 5. Account Registration and Security**

**(1)** The Customer must provide accurate, current, and complete registration information and maintain its accuracy throughout the Subscription Term.

**(2)** The Customer is solely responsible for creating and maintaining the security and confidentiality of their account password and credentials. The Customer shall immediately notify the Provider of any unauthorized access or security breach. The Provider reserves the right to disable any account, username, or password immediately, **with or without prior notice,** if the Customer violates these terms or poses a security risk.

**(3)** The Customer is fully responsible for all activities and compliance of its **Authorized Users** with this Agreement and applicable laws. A violation by an Authorized User is deemed a violation by the Customer.

**Art. 6. License Grant and Operational Limitations**

**(1)** Subject to compliance with this Agreement and fee payment, the Provider grants the Customer a limited, non-exclusive, non-transferable, revocable license to access and use the Platform during the active Subscription Term for the Customer's internal business or personal HR needs only.

**(2)** The Customer acknowledges that all AI Outputs are **advisory in nature** and are intended to support, not replace, human judgment. Final employment decisions (hiring, termination, etc.) must involve meaningful human oversight and validation by qualified professionals.

**(3)** Use of the Platform is subject to technical and operational limitations, which may include restrictions on API calls, data volume, or storage capacity. These limits are detailed in the Customer's account settings and the Service Level Agreement (SLA).

**(4)** The Customer represents that they are not accessing or using the Platform from any jurisdiction subject to comprehensive sanctions imposed by the United States, India, or the European Union.

**Art. 7. Customer Classification and Compliance**

**(1)** The Customer is classified as a **"Consumer"** if acting wholly or mainly outside a trade, business, craft, or profession, benefiting from mandatory consumer protection rights. The Customer is a **"Business Customer"** if using the Platform in connection with a trade or profession, or if the Customer is a company, partnership, or other legal entity.

**(2)** Individual users must be at least eighteen (18) years of age in all jurisdictions. The Platform is not intended for use by minors under eighteen. By registering, you represent and warrant that you are eighteen years of age or older.

**(3)** If the Provider discover that an individual user is under eighteen years of age, will immediately terminate the account and delete all associated data within thirty days, except where retention is legally required. The Provider do not knowingly collect or process personal data of individuals under eighteen.

**(4)** For Business Customers processing employment data, you represent and warrant that all candidates and employees whose data you upload to the Platform are of

legal working age in your jurisdiction. You agree not to upload personal data of individuals under the minimum working age applicable in your region.

**(5) Specific Compliance Requirements:**

1. **India:** Business Customers must comply with the Information Technology Act, the Digital Personal Data Protection Act, and tax regulations (e.g., GST). Consumer rights under the Consumer Protection Act 2019 are retained.
2. **United States:** The Customer is responsible for compliance with Title VII of the Civil Rights Act, EEOC guidelines, the Fair Credit Reporting Act (where applicable), the California Consumer Privacy Act (CCPA), and any state-level AI transparency or bias laws.

**(6)** The Customer is solely responsible for ensuring that their use of the Platform and any reliance on AI Output does not result in unlawful discrimination, bias, or violation of employment, privacy, or data protection laws in their operating regions. The Provider's function is advisory, and final legal liability rests with the Customer as the ultimate decision-maker.

## Section II - Commercial Terms & Subscription Management

### Art. 8 - Billing, Fees, and Overage Transparency

**(1)** The Provider operates a hybrid billing model combining a base subscription fee with usage-based overage charges. The base subscription includes a specified allocation of AI processing requests, data storage, and user seats defined in the Customer's selected plan tier.

**(2)** Usage beyond the included allocation will result in overage fees calculated per unit of excess consumption. Specific usage metrics (e.g., API calls, AI queries, storage volume) and per-unit pricing are prominently displayed in the Customer's account dashboard and pricing page. The Customer will receive automated notifications when usage approaches 75% and 90% of the included allocation.

**(3)** The total accrued overage fees in any given monthly billing cycle shall not exceed two times (2x) the Customer's base subscription fee for that same period. For overage charges exceeding $100 USD (or local currency equivalent) in a month, the Customer must explicitly opt-in to continue usage that would incur such fees.

**(4)** All fees are stated and charged in United States Dollars (USD) unless otherwise specified in the Customer's Order Form. For Customers in India, billing may be conducted in Indian Rupees (INR) at the prevailing exchange rate published by the Reserve Bank of India.

**(5)** The Customer is responsible for all taxes, duties, and governmental assessments arising from this Agreement, excluding the Provider's income taxes. The Provider will collect and remit applicable sales tax, value-added tax (VAT), or Goods and Services Tax (GST) based on the Customer's billing jurisdiction (e.g., India), which will be added to the invoice total. The Customer must provide valid tax exemption certificates where applicable.

**(6)** The Customer must provide valid payment information and authorize the Provider to charge the payment method on file for all fees. Accounts with payment failures exceeding five (5) days may be suspended until payment is received. Late payments accrue interest at the rate of 1 % per month or the maximum rate permitted by law, whichever is lower.

**Art. 9 - Tax Jurisdiction and Collection**

**(1)** Tax jurisdiction is determined by the Customer's billing address for individuals or primary business address for organizations. The Customer is responsible for maintaining accurate address information. Tax rates are calculated based on the address on file when invoices are generated.

**(2)** For Business Customers with India GST registration, the Provider issues GST-compliant invoices with CGST/SGST for intrastate supplies or IGST for interstate supplies. Customers must provide valid GSTIN during registration. Where reverse charge applies, invoices state "Reverse Charge Applicable" and the Customer pays tax directly to government authorities.

**(3)** The Provider collects sales tax in US states where tax nexus exists. Current nexus states are listed on the Provider's website and updated quarterly. Tax-exempt organizations must submit valid exemption certificates to legal@peoplebotapp.com before purchase.

**(4)** All prices displayed on the Platform exclude taxes unless stated otherwise. Invoices show base fees, overage charges, and taxes as separate line items. Customers operating in multiple jurisdictions should contact billing support before subscribing.

**(5)** If the Customer's jurisdiction requires withholding taxes, the Customer may deduct amounts from payments but must provide withholding certificates. The Customer's payment to the Provider plus taxes paid to government must equal the full invoice amount.

**Art. 10 - Overage Fee Notifications and Opt-In Procedures**

**(1)** Usage monitoring and notifications are provided through the following channels:

1. Real-time usage dashboard available in the account showing current consumption against allocation limits;
2. Automated email notifications sent to the account owner's registered email address at 75% and 90% of allocation;
3. Additional email notification when usage reaches 100% of allocation, requiring immediate action.

**(2)** When usage reaches 100% of allocation, the Platform displays a mandatory opt-in prompt before allowing additional usage that would incur overage charges. The prompt clearly shows the per-unit overage rate, estimated cost for the requested additional usage, the monthly overage cap per Art. 8(3), and a checkbox stating "I authorize PeopleBotApp to bill my payment method on file for overage charges according to the rates displayed above." The Customer must affirmatively check the authorization box to continue using services beyond allocation.

**(3)** Once the Customer reaches the monthly overage cap of two times the base subscription fee per Art. 8(3), the Platform automatically suspends overage-triggering features for the remainder of that billing cycle. AI processing requests, new candidate uploads, and automated workflow triggers become unavailable until the next billing cycle begins. Data export, report viewing, account management, and support ticket submission remain available during cap-induced suspension.

**(4)** If the Customer does not provide opt-in authorization when reaching 100% allocation, Platform features are temporarily suspended until the next billing cycle or until opt-in is provided. Suspended features include AI processing requests, new candidate uploads, and automated workflow triggers. Available features during suspension include data export, report viewing, account management, and support ticket submission.

**Art. 11 - Free Trial Provisions**

**(1)** The Provider may offer a free trial period to new customers. The trial duration and feature access are specified during registration.

**(2)** Trial accounts require a valid payment method at activation. No charges are incurred during the trial period. Trial accounts include limited access and reduced usage allocations.

**(3)** At the end of the trial period, the account will automatically convert to a paid subscription and the Customer's payment method will be charged at the applicable plan rate, unless the Customer cancels prior to the expiration of the trial period. The Provider will notify the Customer of the upcoming conversion in advance.

**(4)** Upon trial expiration without upgrade, the account enters a restricted state for ninety (90) days. During this period, the Customer may log in solely to export data or upgrade to a paid subscription. After ninety days, all trial data is permanently deleted from the Platform. The Provider sends reminder emails at sixty, seventy-five, and eighty-eight days after trial expiration.

**Art. 12. Subscription Term Commencement**

**(1)** The Subscription Term is available in monthly or annual billing cycles as selected by the Customer. The initial term begins on the date the Customer completes registration and provides payment information.

**(2)** If the Customer utilizes a free trial, the paid Subscription Term begins immediately upon the Customer's affirmative action to upgrade and provide payment details.

**Art. 13. Automatic Renewal**

**(1)** All subscriptions automatically renew for successive periods equal in length to the original term unless the Customer cancels the auto-renewal before the current period ends.

**(2)** The Provider will charge the Customer's payment method on file at the then-current rate upon each renewal. The Customer explicitly consents to this automatic renewal mechanism.

**(3)** The Provider will send a renewal reminder to the Customer's registered email address at least seven (7) days before each renewal date.

**(4)** Failure to receive a renewal notice does not waive the renewal charge if the Provider made reasonable efforts to deliver it to the Customer's last known email address. The Customer is responsible for keeping their contact information current.

**Art. 14. Free Trial Conditions and Restrictions**

**(1)** The Provider offers one free trial period per individual or legal entity (organization) that has not previously used the Platform. Trial duration is specified during registration.

**(2)** Free trials require a valid payment method to activate. No charge is made during the trial period. The Customer may explore limited Platform features during the trial. If the Customer does not cancel prior to the expiration of the trial period, the Customer's payment method will be charged automatically in accordance with Art. 14(4).

**(3)** The Provider reserves the right to deny or immediately terminate a free trial if the Provider determines, in its reasonable judgment, that the Customer is abusing the trial offering. Abuse includes:

1. Attempts to register multiple trial accounts associated with the same corporate or organizational domain name.
2. Registration using temporary, disposable, or invalid email addresses.

**(4)** Trial accounts automatically convert to paid subscriptions upon expiration of the trial period. The Customer's payment method on file will be charged at the applicable plan rate unless the Customer cancels the trial prior to its expiration. Cancellation may be performed through the Customer's account settings or by contacting the Provider's support team.

**(5)** If the Customer does not upgrade before trial expiration, the account enters a restricted state for ninety (90) days. The Customer retains login access solely for data export purposes during this period. All trial data is permanently deleted after ninety days if no paid subscription is activated. The Provider is not liable for data loss after the ninety-day retention period expires.

**Art. 15 - Upgrades and Downgrades**

**(1)** The Customer may upgrade their subscription plan at any time. Upgrades take effect immediately, and the Provider will calculate a prorated credit for the unused portion of the current term and apply it toward the new plan's cost.

**(2)** The Customer may downgrade their subscription plan at any time, but the downgrade will take effect only at the end of the current billing cycle. No refunds or credits are provided for the period between the request and the effective date.

**(3)** The Customer is responsible for reducing usage (e.g., removing Authorized Users or stored data) to comply with the lower-tier plan's limits before the downgrade becomes effective.

**Art. 16 - Cancellation and Termination by Customer**

**(1)** The Customer may cancel their subscription and disable auto-renewal at any time through the account dashboard. Cancellation is processed immediately, but access to the Platform continues until the end of the current paid billing period.

**(2)** Cancellation does not entitle the Customer to a refund for the current billing period unless the Customer qualifies under the specific refund conditions detailed in **Art. 28-31** (Refund Policy section)

**(3)** Following termination, Customers have thirty days to retrieve and export all Customer Data as specified in **Art. 43-45**

### Art. 17 -Modification of Terms and Pricing

**(1) The Provider** reserves the right to modify subscription plan features, pricing, or allocations at any time. Changes to pricing or material reductions in functionality require at least fourteen (14) days' advance written notice to active subscribers.

**(2)** Price increases and material feature changes apply only to renewal periods following the notice, not to the Customer's current Subscription Term. If the Customer does not accept the modified terms or pricing, the Customer may cancel the subscription before the renewal date without penalty.

**(3)** The Provider may discontinue or substantially modify subscription tiers with thirty (30) days' advance notice. If the Customer's current plan is discontinued, the Provider will offer the option to migrate to the most comparable available plan or to cancel the subscription with a prorated refund for any unused portion.

## Section III -Rights, Obligations & Acceptable Use

### Art. 18 - Customer Rights During Active Subscription

**(1)** Every Customer using the Platform has the following rights during an active Subscription Term:

1. Access to all features and functionality included in the subscribed plan tier;
2. Full ownership of all Customer Data uploaded to or created within the Platform;
3. Right to export Customer Data at any time in machine-readable formats through the account dashboard;
4. Technical support according to the response times specified for the subscription level;
5. Right to request general information about how the AI Co-Pilot processes inputs and generates recommendations;
6. Right to submit complaints and request investigation under the Service Level Agreement when Platform malfunctions occur;
7. Right to cancel the subscription at any time through the self-service cancellation function.

**(2)** Business Customers with enterprise-tier subscriptions receive these additional rights:

1. Designation of multiple Authorized Users with differentiated permission levels and role-based access controls;
2. Priority technical support with faster response times during business hours;
3. Right to audit the Provider's security practices and review relevant compliance certifications upon reasonable request with appropriate confidentiality protections;
4. Access to dedicated technical account management for accounts processing significant volumes of sensitive employment data, subject to additional fees where applicable;
5. Ability to request custom integration support and advanced API access beyond standard offerings.

**Art. 19 - Customer Obligations and Compliance Requirements**

**(1)** Every Customer must fulfill the following obligations when using the Platform:

1. Provide accurate and complete information during registration and maintain current account details;
2. Safeguard login credentials and prevent unauthorized access to the account;
3. Use the Platform only for lawful purposes in compliance with all applicable laws, including employment regulations, data protection requirements, and anti-discrimination statutes;
4. Obtain all necessary consents and legal authorizations before uploading candidate information, employee records, or other personal data;
5. Implement human oversight when using AI-generated recommendations for employment decisions;
6. Refrain from relying solely on automated outputs to make hiring, promotion, or termination choices;
7. Pay all fees when due and maintain valid payment information on file;
8. Notify the Provider immediately upon discovering unauthorized account access or security breaches.

**(2)** Business Customers bear these heightened responsibilities:

**1.** Ensure all Authorized Users under the account comply with these terms and the Acceptable Use Policy, as violations by any user are attributed to the organization;
**2.** Conduct independent bias audits and fairness assessments of AI outputs before implementing them in employment processes, particularly where regulations require such validation;

3. Ensure compliance with employment laws in each jurisdiction where the Platform processes candidate or employee data;
4. Maintain adequate internal documentation of human review processes to demonstrate compliance with laws prohibiting solely automated decision-making;
5. Implement appropriate mechanisms to inform candidates and employees that AI assists in processing their information;
6. Provide channels for individuals to request human-only review where legally required under GDPR Article 22, India DPDP Act, or similar legislation.

**Art. 20 - Provider Rights and Platform Control**

**(1)** The Provider has the following rights in relation to Platform operation and Customer accounts:

1. Right to modify, update, or enhance Platform features at any time without prior notice, provided core functionality included in the Customer's subscription tier is not materially diminished;
2. Right to monitor account usage patterns using automated systems to detect violations of these terms, including data scraping, competitive intelligence gathering, or reverse engineering attempts;
3. Right to immediately suspend account access when suspected terms violations, security threats, or unlawful activity are detected;
4. Right to refuse service to any individual or organization that has previously violated these terms, engaged in fraudulent activity, or poses unreasonable legal or security risk;
5. Right to decline reinstatement of suspended accounts even after violations are remedied if the risk of future violations remains unacceptably high;
6. Full ownership of all intellectual property in the Platform, including software, algorithms, user interface designs, documentation, and branding;
7. Right to use anonymized and aggregated data derived from customer usage patterns to improve services, train models, and develop new features, provided such use does not reveal information about any specific Customer or compromise confidentiality.
8. Right to engage sub-processors and third-party service providers to assist in delivering Platform services, subject to notification requirements specified in these terms;
9. Right to adjust rate limits, usage quotas, or access controls to ensure fair resource allocation and system stability for all customers;
10. Right to require immediate plan upgrade or throttle account access when usage patterns significantly exceed normal parameters for the subscription level;

11. Right to conduct remote usage audits of Business Customer accounts to verify compliance with subscription terms and license limitations.

**Art. 21 - Provider Service Delivery Obligations**

**(1)** The Provider has the following obligations to all Customers during active Subscription Terms:

1. Maintain the Platform in operational condition according to uptime standards specified in the Service Level Agreement;
2. Implement and maintain commercially reasonable security measures to protect Customer Data from unauthorized access, including encryption in transit and at rest;
3. Notify the Customer within seventy-two hours if a data breach affecting the Customer's account is discovered, including details about the nature of the breach, categories of data affected, and remediation steps being taken;
4. Process Customer Data only in accordance with instructions provided through Platform use and as necessary to deliver contracted services;
5. Refrain from using Customer Data to train AI models or for any purpose beyond service delivery unless the Customer provides explicit opt-in consent through account settings.
6. Provide reasonable advance notice before making material changes to these terms, pricing, or core Platform functionality that significantly restrict Customer rights, expand Customer obligations, or alter fundamental service characteristics;
7. Cooperate with valid legal process where required by law while notifying the Customer of such requests where legally permitted so the Customer may seek protective orders.
8. Provide at least thirty days' notice before new sub-processors begin processing personal data, giving Customers time to object if arrangements create concerns;
9. Respond to Customer support requests within timeframes specified for the applicable subscription tier;
10. Provide access to general information about AI processing methodologies upon Customer request, subject to protection of proprietary algorithms and trade secrets;

**Art. 22 - Anti-Discrimination Requirements**

**(1)** Customers are strictly prohibited from using the Platform in ways that violate employment or anti-discrimination laws. This includes using AI outputs to automatically reject candidates based on protected characteristics.

**(2)** Protected characteristics include race, color, religion, sex, national origin, age, disability status, genetic information, or any other classification protected under applicable law. Customers may not configure the Platform to discriminate based on these factors.

**(3)** Customers may not use AI recommendations as the sole basis for adverse employment actions. All hiring rejections, promotion denials, termination decisions, and compensation determinations must involve meaningful human review by qualified personnel.

**Art. 23 - Customer Data Quality and Compliance Obligations**

**(1)** The Customer must ensure all data uploaded to the Platform is accurate, current, and in readable formats. This includes candidate resumes, job descriptions, employee records, and company information. The Customer is responsible for regularly updating uploaded data to maintain accuracy.

**(2)** The Customer represents that all data uploaded to the Platform was lawfully collected and that the Customer possesses all necessary rights to process such data. Where privacy laws require candidate or employee consent before AI processing, the Customer must obtain that consent before uploading personal data. The Customer may not upload data obtained through illegal means, unauthorized access, or in violation of confidentiality obligations.

**(3)** AI output quality depends directly on input data quality. If the Customer provides incomplete, outdated, or poorly formatted data, AI recommendations may be unreliable or unusable. The Provider is not responsible for poor results stemming from deficient input data.

**(4)** The Customer is prohibited from uploading data containing known discriminatory patterns or biased information. If the Customer discovers data inputs may be producing biased outputs, the Customer must immediately cease using those outputs and notify legal@peoplebotapp.com. The Customer may not use the Platform to circumvent employment verification or background check requirements.

**(5)** The Customer must inform candidates and employees that AI technology assists in processing their information. This notification must occur at or before data collection. Where required by law, the Customer must provide candidates with a mechanism to request human-only review or object to automated processing.

**Art. 24 - Prohibited Data Scraping and Competitive Use**

**(1)** Customers are expressly prohibited from engaging in data scraping, web crawling, automated data extraction, or similar activities that systematically copy information

from the Platform. Customers may not use robots, scripts, or automated tools to access the Platform except through official API endpoints.

**(2)** Customers may not use the Platform to develop, benchmark, or improve competing products or services. This prohibition includes both direct competition in the HR technology space and derivative uses that would disadvantage the Provider's market position. Violation of data scraping or competitive use restrictions constitutes material breach. The Provider may immediately terminate the account without refund and pursue additional remedies including injunctive relief and monetary damages.

**Art. 25 - Third-Party Service Integrations**

**(1)** The Platform integrates with various third-party services and applications to enhance functionality. These may include calendar systems, communication platforms, applicant tracking systems, or human resources information systems.

**(2)** When a Customer authorizes integration with a third-party service, that service may access certain Customer Data necessary for the integration to function. Data shared with third-party services becomes subject to those providers' own terms and privacy policies.

**(3)** The Provider disclaims responsibility for outages, data loss, security breaches, or functionality problems caused by third-party service providers. Such incidents are not treated as breaches of the Service Level Agreement unless caused by the Provider's systems.

**(4)** Customers must comply with terms of service for any third-party platforms integrated with the Platform. Violations of third-party terms that result in revoked API access are the Customer's responsibility.

**Art. 26 - Rate Limits and Usage Quotas**

**(1)** Customer use of the Platform is subject to reasonable rate limits and usage quotas. These limits ensure fair resource allocation and system stability for all customers. Specific limits vary by subscription tier and are documented in the account dashboard.

**(2)** If Customer usage patterns significantly exceed normal parameters for the subscription level, the Provider reserves the right to throttle the account temporarily or require upgrade to a higher-tier plan. The Provider will notify the Customer before implementing throttling measures except where excessive usage threatens system stability.

**(3)** Sustained usage far exceeding plan allocation may be treated as evidence of inappropriate use. In such cases, the Provider may require immediate plan upgrade or suspend service until usage patterns normalize.

### Art. 27 - Usage Audits for Business Customers

**(1)** Enterprise and professional-tier Business Customers may be subject to periodic usage audits to verify compliance with subscription terms. The Provider may conduct remote audits by reviewing system logs, usage metrics, and account configuration.

**(2)** Audit requests will be made in writing with at least fourteen days' notice. Customers agree to cooperate by providing reasonable access to usage information and allowing review of Authorized User account configuration.

**(3)** All information gathered during audits is treated as confidential. If an audit reveals usage exceeding the subscription level, the Customer has thirty days to upgrade or reduce usage to compliant levels before the Provider takes enforcement action.

**(4)** Audits will not be conducted more frequently than once per calendar year unless specific evidence suggests ongoing compliance violations. Audit costs are borne by the Provider unless the audit reveals usage exceeding the plan by more than twenty percent.

## Section IV -Refund Policy

### Art. 28 - Refund Policy Overview

**(1)** The Provider shall only refund subscription fees under the specific conditions outlined in this Article and Art. 29-31. The Provider does not refund subscription fees based solely on customer dissatisfaction, change in business needs, or subjective quality assessments.

**(2)** The Provider shall not issue refunds for subscription fees based solely on the Customer’s determination that the Platform is not a fit for them. The Provider also will not issue refunds because the AI Output did not meet the Customer’s subjective expectations at the time of purchase or if the Customer changes their mind after the purchase.

### Art. 29 - Refund Eligibility Conditions

**(1)** A Customer can request a refund when, through the execution of appropriate documentation, the Customer has been unable to utilise core functions of the Platform due to a documented malfunction of the Platform for an extended period

of time. This malfunction must inhibit the Customer's means of utilising the Platform as intended.

**(2)** Refunds are appropriate when the Provider has violated the Service Level Agreement's (SLA) commitment to uptime and availability, and this violation meets the threshold conditions contained in the SLA for the Customer to be eligible for consideration for a refund from the Provider.

**(3)** In order for an issue to qualify as a malfunction that warrants a refund, the malfunction must meet the criteria listed above, including:

1. The malfunction must have a significant effect on the Customer's ability to use the Platform for its intended purpose, and
2. If the Customer reports a malfunction, the Provider will determine, based on technical assessment, whether the malfunction qualifies as a malfunction warranting refund consideration.

**(4)** Examples of issues that are not considered malfunctioning to the extent necessary to warrant refund consideration include:

1. Slowness of Platform performance(i.e., Platform response times) or
2. Minor bugs or temporary inconvenience.

**Art. 30 - Refund Request Procedures**

**(1)** Customers must submit refund requests in writing through the support ticket system or specified refund request email address. Such requests should be filed within thirty days of the incident that forms the basis of the refund claim.

**(2)** The following information is required for each request for refund:

1. Specific dates and times when the malfunction or SLA breach occurred;
2. A detailed description of the problem experienced, including error messages or symptoms;
3. Supporting documentation/evidence for the claim, including screenshots, system logs, or correspondence with support staff;
4. Explanation of how the issue prevented use of the Platform and impacted the Customer's operations.

**(3)** Provider will investigate all properly submitted refund requests and respond within fifteen business days. The response will indicate whether the refund request is approved, partially approved or denied along with explanation of the decision.

**Art. 31 - Refund Calculation and Processing**

**(1)** Refunds approved are pro-rated. The amount of the refund is calculated based on the percentage of the subscription period where the Platform has been unavailable or not operational because of the relevant malfunction.

**(2)** Refund amounts are limited to fees paid during the period directly affected by the malfunction or SLA breach. Total refunds cannot exceed the amount paid in the three months immediately preceding the refund request submission.

**(3)** Annual subscription refunds are pro-rated by dividing the annual fee by twelve in order to come up with the relevant monthly equivalent rate. After that, the pro-rated refund is calculated based on how many days the Platform was unavailable during the affected month.

**Art. 32 - Refund Processing and Payment Methods**

**(1)** Refunds approved will be returned to the payment method that the subscription was purchased with. Refunds will be processed within thirty (30) days of the refund being approved by the Provider.

**(2)** If the original payment method is no longer valid for purchase due to expiration or other reasons, the Customer must provide alternative instructions on how to receive a refund. The Provider reserves the right to request any additional documentation to verify the refund if the refund method is different from the method used for the purchase.

**(3)** Under the terms of the Agreement, Refunds issued by the Provider are the only remedy and option available to Customers for claims arising from platform malfunction or the Provider's failure to meet its Service Level Agreement (SLA). The acceptance of a refund will satisfy and close any claims related to the platform or SLA malfunction.

**Art. 33 - Consumer Protection Rights (EU and India)**

**(1)** Consumer Customers who are located in the European Union may have rights to withdraw from the Contract within fourteen (14) days of its conclusion under the Consumer Rights Directive; however, these rights are being waived when the Customer specifically consents to the Provider performing the services before the expiration of the fourteen (14) day period, and that by consenting to immediate service, the Customer is losing their withdrawal rights.

**(2)** Individual customers in India using the Platform for personal purposes unrelated to business are "consumers" under the Consumer Protection Act 2019 and possess non-waivable statutory rights. Consumers may file complaints before Consumer Disputes Redressal Commissions for defective or deficient service. Jurisdictional

thresholds are: District Forum for claims up to ₹1 crore, State Commission for claims from ₹1 crore to ₹10 crore, and National Commission for claims exceeding ₹10 crore.

**(3)** The mandatory arbitration provision in Art. 80 does not apply to Indian consumers protected by the Consumer Protection Act. Consumers may choose to file complaints before Consumer Forums or voluntarily agree to arbitration. Once proceedings begin in either forum, that choice binds that dispute. Service of consumer forum notices should be directed to legal@peoplebotapp.com.

**(4)** While Consumer Protection Act rights cannot be waived, certain limitations under these terms remain enforceable to the extent permitted by law. Liability caps per Art. 73 may limit monetary compensation. Refund eligibility conditions per Art. 29-31 refund eligibility criteria apply to refund requests regardless of forum. The Provider commits to responding to consumer forum notices promptly and complying with forum orders.

**(5)** Business Customers using the Platform for trade, business, or professional purposes are not "consumers" under the Consumer Protection Act 2019. Business Customers may not file complaints before Consumer Forums and must follow dispute resolution procedures in Art. 80. This ensures commercial disputes are resolved through appropriate business channels while preserving individual consumer protections.

**Art. 34 - Business Customer Refund Limitations**

**(1)** Business customers are not entitled to the consumer protection refund rights described in the preceding Article 33. Business customers are only entitled to receive refunds in the event of a malfunctioning platform and/or breach of SLA as specified in Articles 29 through 32.

**(2)** Business customers who cancel their subscriptions for convenience shall not receive a refund for the remnant of the prepaid subscription period, as the subscription will continue to be in effect and available for use until the end of the prepaid period.

**Art. 35 - Non-Refundable Circumstances**

**(1)** There shall be no refunds for subscription fees if the customer breaches the Terms and Conditions or the Acceptable Use Policy, and the provider terminates the customer's account for cause. The account of a customer that has been terminated for cause shall not be entitled to a refund of any prepaid fees.

**(2)** Refunds are not extended where problems with the functionality of the Platform arise from the Customer's own actions: inability to access the Internet, insufficient

browser or other device compatibility, failure to maintain compatible systems, or an inability to use Platform features due to user error.

**(3)** No refunds are issued in the case of unavailability due to circumstances beyond the Provider's reasonable control, including any force majeure events, third-party service provider outages, Internet backbone failures, and/or distributed denial-of-service attacks.

**(4)** Usage-based overage fees are non-refundable under any circumstance. Any fees associated with AI processing requests, API calls, or other metered services are considered earned and non-refundable once consumed, regardless of subsequent account status.

### Art. 36 - Consumer Statutory Rights Preservation

**(1)** Nothing in this refund policy limits the Customer's right to pursue legal remedies for fraud, gross negligence, or intentional misconduct by the Provider. Customers retain all statutory rights that cannot be waived under mandatory consumer protection laws in their jurisdiction.

**(2)** This refund policy is not connected with, and does not interact with, any service credit that may be due under the Service Level Agreement. Customers may receive SLA credits but not monetary refunds, in accordance with the SLA document. This refund policy does not provide for monetary refunds where SLA service credits are the appropriate remedy. For SLA credit provisions, refer to Art. 78.

## Section V -Termination & Account Closure

### Art. 37 - Termination for Cause by Provider

**(1)** The Provider may terminate a Customer's account immediately if there is a material breach of these terms by the Customer, and the latter fails to remedy the infringement within seven days of receiving a written notice by email. Material breaches include but are not limited to:

1. Non-payment of fees when due, including subscription charges and overage amounts;
2. Violation of the Acceptable Use Policy, be it prohibited HR uses or data scraping activities;
3. Unauthorized attempts to access, breach, or compromise the security of the Platform;
4. Using the Platform for unlawful purposes or in such a way that gives rise to legal claims against the Provider;
5. Supplying false information upon registration or during account updating;
6. Transfer or assignment of the account to third parties without the written consent of the Provider.

**(2)** Where the breach cannot reasonably be cured, the Provider may terminate immediately without an opportunity to cure. Events involving fraud, crime, and violations which create an immediate security threat to the Platform or another customer are illustrative of such.

**Art. 38 - Termination Due to Insolvency**

**(1)** The Provider may terminate account(s) for customers if they file for bankruptcy, enter into receivership, insolvency proceedings, or any other court action that adversely affects the customer's ability to make payments as required under the contract.

**(2)** Termination will take effect thirty (30) days after the Provider sends a written notice to the customer's registered address unless the customer enters into an alternate agreement to continue payment during this period.

**(3)** A termination will also be effective if either party ceases to do business materially, liquidates, or has a receiver appointed with respect to all or substantially all of its assets. A written notice must be provided, and termination will be effective fifteen (15) days after delivery.

**Art. 39 - Account Suspension**

**(1)** Accounts automatically enter suspended status if subscription fees or overage invoices remain unpaid for fifteen days beyond the due date. During suspension, the Customer may only access account login, payment updates, and balance payment functions. Access restores within twenty-four hours after payment is received.

**(2)** The Provider may immediately suspend accounts when detecting suspicious activity requiring investigation. This includes unusual login patterns, suspected compromises, data scraping attempts, or malicious code uploads. Suspension remains until investigation completes and the Provider receives satisfactory explanations from the Customer.

**(3)** When implementing security-related suspension, the Provider notifies the Customer within twenty-four hours via email. The Customer must respond to investigation requests within seven days, which may include identity verification, activity explanations, or password resets. Failure to cooperate may result in permanent termination per Art. 37.

**(4)** Suspended accounts may be reactivated once the underlying issue is resolved. Payment suspensions reactivate automatically upon payment clearance. Security suspensions require successful investigation completion and implementation of

required security measures. The Provider has no obligation to reactivate accounts where violations are confirmed or security risks remain.

**Art. 40 - Reactivation Procedures**

**(1)** Suspended accounts may, upon the Customer's initiative, be reactivated when the root cause has been eliminated. In the event of any payment-related suspension, once valid payment information has been provided and all outstanding sums are settled, access will be restored within twenty-four hours.

**(2)** In cases of security-related suspensions, the Customer will respond to Provider's requests for investigation and prove that their account has not been compromised. Additional verification steps may be necessary, including confirmation of identity or password resets.

**(3)** Provider is under no duty to reinstate accounts where investigation reveals violations of these Terms or where the Customer fails to cooperate with reasonable verification requests. Suspension may be lifted at the discretion of the Provider and converted to permanent termination.

**Art. 41 - Effect of Termination on License and Fees**

**(1)** Upon termination by either the Customer's or the Provider's initiation, the license to access and use the Platform shall immediately terminate. The Customer shall immediately cease all use of the Platform and shall not attempt to access the account at any time, except as may be specifically permitted for data retrieval purposes.

**(2)** Termination does not relieve either party from obligations to pay all accrued service fees through the effective date of such termination, including subscription charges, overage fees, and other amounts properly invoiced hereunder.

**(3)** Prepaid fees for periods extending beyond the termination date are not refunded except in cases where the Provider terminates without cause or where mandatory consumer protection laws require refunds. Business Customers terminating for convenience receive no refund for unused prepaid periods.

**Art. 42 - Survival of Obligations After Termination**

**(1)** Termination does not affect obligations that logically should continue after the relationship ends. These surviving provisions include confidentiality commitments, intellectual property rights, liability limitations, indemnification duties, and dispute resolution procedures.

**(2)** All warranties and disclaimers made before termination remain effective and apply to all AI-generated outputs and services provided up until the time of

termination. A customer cannot later assert that AI recommendations issued during an active subscription were inadequately disclosed simply because the subscription has been terminated.

**(3)** The obligation of the Provider to assist with retrieval requests for data will survive termination as specified by Article 44. The Provider will no longer have any obligation to assist with Customer Data after the retrieval time period has closed.

**Art. 43 - Customer Data Retrieval Window**

**(1)** Following termination, Customers have thirty days to retrieve and export all Customer Data stored in the Platform. This retrieval window begins on the effective termination date, whether termination was initiated by the Customer or the Provider.

**(2)** During the retrieval period, the Customer may log into the account with limited access specifically for data export purposes. The self-service export function in the account dashboard remains available, allowing download of Customer Data in machine-readable formats including CSV, JSON, and PDF depending on data type.

**(3)** For Business Customers with large data volumes, the Provider can arrange bulk data transfer via secure file transfer protocol. Requests for bulk transfer must be submitted within the first fifteen days of the retrieval period to allow adequate processing time.

**Art. 44 - Data Deletion Timeline and Procedures**

**(1)** The Provider maintains Customer Data in a retrievable state throughout the thirty-day retrieval window. After this period expires, the Provider will permanently delete all Customer Data from active systems and backups.

**(2)** Permanent deletion occurs within sixty days after the retrieval period ends. The Provider uses industry-standard data destruction practices to ensure deleted data cannot be recovered through any technical means.

**(3)** The Provider may retain certain limited information beyond the deletion timeline only where required by law, regulatory mandate, or legitimate legal purposes such as defending against potential claims. Any retained information is maintained under strict confidentiality and security controls equivalent to those applied during active service delivery.

**Art. 45 - Customer Responsibility for Data Export**

**(1)** Customers are solely responsible for exporting their data before the retrieval window closes. The Provider sends automated reminder notifications at the beginning of the retrieval period and again at fifteen days before expiration.

**(2)** Failure to export data within the permitted timeframe results in permanent loss of that data. The Provider bears no liability for data loss that occurs because the Customer did not take advantage of the retrieval period. This includes situations where the Customer forgot about the deadline, experienced technical difficulties on their end, or simply chose not to export.

**(3)** The Provider will not extend retrieval periods or restore deleted data under any circumstances once the ninety-day window expires. The Customer is solely responsible for exporting data before the deadline. The Provider bears no liability for data loss resulting from the Customer's failure to export data during the retrieval period.

### Art. 46 - Account Reactivation After Termination

**(1)** Customers who terminate and later wish to reactivate may create new accounts by completing the standard registration process. Reactivation is treated as a new subscription and does not restore any data that was deleted following the previous termination.

**(2)** The Provider reserves the right to decline new registrations from individuals or organizations whose previous accounts were terminated for cause. Past violations of these terms may result in permanent exclusion from Platform access.

## Section VI -Intellectual Property & AI Framework

### Art. 47 - Customer Data Ownership and Processing License

**(1)** The Customer retains full ownership of all Customer Data uploaded to or created within the Platform. This includes candidate resumes, employee records, job descriptions, company information, and any other content the Customer provides.

**(2)** Customer hereby grants to Provider a limited license to process Customer Data solely to deliver the services provided through the Platform and only for the duration of the Subscription Term. This license shall terminate upon the expiration of the Subscription Term.

**(3)** The Provider shall not use Customer Data to train AI models, improve algorithms, or develop new features unless the Customer explicitly provides opt-in consent via account settings. This restriction is absolute and applies without exception, even if data is anonymized.

### Art. 48 - AI Output Ownership and IP Transfer

**(1)** The Customer shall retain all intellectual property rights in the output generated through the AI with respect to job descriptions, candidate summaries, draft policies,

interview questions, and any other text created by the AI Co-Pilot in response to Customer input. However, AI outputs may not always qualify for copyright protection under applicable law. Some AI-generated content may fall into the public domain or lack sufficient originality for copyright registration. The Customer acknowledges this limitation and assumes all risks related to the IP status of AI outputs.

**(2)** The Provider may use anonymized and aggregated data from patterns of AI processing. Such aggregated data does not include any information traceable to any given Customer and serves exclusively to enhance Platform functionality and provide new features.

**Art. 49 - Third-Party AI Model Provider Terms**

**(1)** The Platform uses AI models from third-party technology companies, including OpenAI and Anthropic. These providers retain certain rights in their underlying AI technology as specified in their respective terms of service.

**(2)** While the Customer owns AI outputs generated through the Platform, those outputs remain subject to the usage policies of the underlying AI providers. Customers are required to use AI-generated content in compliance with the OpenAI Usage Policies and Anthropic Usage Guidelines.

**(3)** Provider specifically disclaims any warranty that AI Outputs are free from third-party intellectual property claims. Results generated by AI may incidentally resemble existing works. It is the Customer's sole responsibility to check that AI Outputs do not infringe on third-party rights before making public or commercial use thereof.

**Art. 50 - Platform Intellectual Property Rights**

**(1)** All intellectual property rights with respect to the Platform itself, including but not limited to software code, algorithms, machine learning models, user interface designs and visual elements, documentation and training materials, brand assets are proprietary to the Provider.

**(2)** Customers are granted no proprietary rights in the Platform technology. The license that is granted by Section I is to access and use the Platform as a service and not to obtain proprietary rights in the underlying systems themselves.

**(3)** The Customer shall not reverse-engineer, decompile, disassemble, or otherwise try to extract source code from the Platform. Nor may the Customer copy, modify, adapt, or create derivative works of any Platform technology.

**Art. 51 - Beta Features and Experimental Functionality**

**(1)** Every so often, the Provider releases or may release features in beta, experimental functionality, or early-access capabilities. These features are clearly marked as beta or preview within the Platform interface.

**(2)** Beta features are provided "as-is" without any warranty or guarantee of any kind. The Provider does not commit that beta features will work reliably, remain available or ever be released as standard features.

**(3)** Beta features are expressly excluded from Service Level Agreement commitments. No outages, bugs, or poor performance in beta functionality constitute SLA breaches, or grounds for refunds or service credits.

**Art. 52 - Customer Feedback and Improvement License**

**(1)** In the event that Customers submit any remarks, suggestions, ideas concerning the improvement of the Platform, the Provider is granted a perpetual, irrevocable, worldwide license to utilize such feedback without any limitation or remuneration.

**(2)** This feedback license permits the Provider to act upon suggestions, include ideas in product development and share concepts with other customers, all without any payment obligation to the original submitter. Customers hereby waive all intellectual property claims over feedback voluntarily submitted to Provider and/or its affiliates.

**Art. 53 - AI Model Updates and Version Changes**

**(1)** The Provider is entitled to update the AI models at any time with a view to optimizing performance, precision, or functionality. Changes in models can produce differences in output quality, style, or characteristics within previously obtained results.

**(2)** Provider does not warrant that AI outputs are backward compatible across different versions of the models. Outputs created pre-update will potentially differ from created outputs post-update for the same input.

**(3)** Whenever reasonably possible, the Provider shall provide thirty days' notice in advance of significant changes to AI models. Minor tuning, bug fixes, or incremental improvements can be deployed at any time without prior notice.

**Art. 54 - AI Training Data Sources**

**(1)** Publicly available information, licensed data sets and proprietary information developed by the Provider and its technology partners. Specific details regarding the training data shall be considered as confidential trade secrets.

**(2)** Provider does not use Customer Data to train any AI, unless a customer explicitly opts in within account settings. This commitment applies regardless of whether Customer Data would be anonymized before training use.

### Art. 55 - Commercial Rights in AI Outputs

**(1)** Customers can use, modify, adapt, and commercialize AI output in any way they think fit in the Platform. No further charges, royalties, or permissions are payable beyond the subscription charges that have already been made.

**(2)** Customers are solely responsible for ensuring that their use of AI outputs complies with applicable law and should verify separately before implementation that such outputs do not infringe third-party rights, violate employment regulations, or contain discriminatory content.

## Section VII -AI Governance Summary

### Art. 56 - AI System Classification and Risk Level

The AI functionality of the Platform is designed and operated for the purpose of a recommendation engine and co-pilot tool, rather than a high-risk automated decision-making system in accordance with the EU AI Act or similar legislation. All AI outputs shall be advisory in nature and require human review before implementation in employment decisions.

### Art. 57 - Human Oversight Requirements

**(1)** Customers shall use meaningful human oversight if they rely upon an AI-generated recommendation for any employment-related purpose, including making decisions with regard to hiring, candidate selection, evaluation, promotion, or termination.

**(2)** AI outputs cannot be used as the sole basis for taking adverse employment actions. Qualified personnel have to review AI recommendations, taking into account individual circumstances and context, and exercising independent judgment before making the final decisions.

**(3)** Business Customers must maintain sufficient records of their human review processes. These records may be required in order for the Business Customer to demonstrate compliance with laws prohibiting purely automated decision-making in jurisdictions such as the European Union, India, and several U.S. states.

**(4)** The Provider provides technical tools to support human oversight requirements, including features for audit logging when and how AI recommendations are

reviewed. However, implementing appropriate review procedures remains exclusively the Customer's responsibility.

**Art. 58 - AI Governance and Transparency**

**(1)** Details regarding the Provider's AI governance practices, selection criteria for models, mitigation of bias, and transparency are set forth in its separate AI Transparency & Use Policy. This policy is hereby incorporated into this agreement by reference and can be accessed via the website of the Provider and from the account dashboard of the Customer.

**(2)** The AI Policy encompasses such issues as algorithmic testing of fairness, sources and limitations of training data, procedures for model updates, explainability features, mechanisms of incident reporting. Customers are encouraged to review the AI Policy in order to understand how the Platform processes data and makes recommendations.

**Art. 59 - AI Bias Disclaimer and Customer Validation**

**(1)** Irrespective of the commercially reasonable effort to reduce algorithmic bias, the Provider does not warrant that AI outputs shall be free from bias inaccuracy or error. In general AI models may reflect biases due to the training data and model architecture or due to reasons beyond Providers' control.

**(2)** The Customer is solely responsible for ensuring AI outputs comply with anti-discrimination and employment laws before implementation. This includes conducting independent bias audits, monitoring for disparate impact, and implementing corrective measures if bias is detected. The Provider is not responsible for discriminatory outcomes resulting from the Customer's use of AI outputs without adequate validation.

**(3)** Accordingly, the Supplier excludes liability for any claims under employment discrimination, regulatory fines, brand damage, or third-party claims resulting from use of the output provided by AI. Customers shall not depend on any recommendations given by AI without proper validation and human judgment.

**(4)** In the case of detecting suspected bias in AI output, the Customer should notify the Provider's AI ethics team. Such notifications will be researched and, where possible, appropriate adjustments will be made. No commitment is provided to revise models based on an individual report.

**Art. 60 - Right to Object to AI Processing**

**(1)** Candidates and employees whose information is processed through the platform may have legal rights to object to automated processing under the GDPR Article 22, India Digital Personal Data Protection Act, or similar legislation. Customers must

implement mechanisms allowing individuals to exercise these rights where legally required.

**(2)** The Provider offers technical features supporting the right-to-object requirements, such as the capability to flag certain candidate records only for human review or to withhold data from AI processing. Customers are expected to continue communicating the existence of this right with candidates and providing them with a channel for their objection requests.

### Art. 61 - AI Transparency and Reporting

**(1)** Upon reasonable request, the Provider will provide general information about AI processing methodologies, including types of models used, categories of data processed, and general decision-making logic. However, proprietary algorithms, specific model weights, and detailed training data remain confidential.

**(2)** Enterprise-tier Business Customers may request more detailed AI transparency reports subject to appropriate confidentiality protections and possible additional fees. These reports can include information such as bias testing results, model performance metrics, and processing audit trails relevant to the Customer's specific use case.

## Section VIII -Data Protection & Security

### Art. 62 - Data Protection Framework

**(1)** The Provider's Privacy Policy governs all aspects of personal data collection, processing, storage, and protection in connection with Platform use. The Privacy Policy is an integral part of these Terms & Conditions and is incorporated by reference as if fully set forth herein.

**(2)** The Privacy Policy is accessible through the Provider's website and within the Customer's account dashboard. Customers must review the Privacy Policy to understand how personal data is handled, what rights data subjects possess, and how privacy-related requests should be submitted.

**(3)** The Provider processes personal data in compliance with applicable data protection laws, including the EU General Data Protection Regulation, the India Digital Personal Data Protection Act 2023, the California Consumer Privacy Act, and other relevant privacy legislation in jurisdictions where the Platform operates.

**(4)** For Business Customers who upload personal data of candidates or employees, a separate Data Processing Addendum defines the parties' roles and obligations as data controller and data processor. The DPA includes Standard Contractual Clauses

for international data transfers, security requirements, sub-processor management, and data subject rights fulfillment procedures.

**Art. 63 - Data Security Standards and Certifications**

**(1)** The Provider implements commercially reasonable technical and organizational security measures to protect Customer Data from unauthorized access, disclosure, alteration, or destruction. Security controls include encryption of data in transit and at rest, multi-factor authentication options, role-based access controls, regular security assessments, and continuous monitoring for threats.

**(2)** The Platform is hosted on AWS infrastructure with default hosting in US regions (US-East-1 and US-West-2). For Business Customers requiring India data localization under the DPDP Act, the Provider offers India-region hosting on AWS Mumbai (ap-south-1) infrastructure. India-region hosting is available for all subscription tiers and can be activated within sixty (60) days of account creation or upon request.

**(3)** India-region hosting incurs an additional fee of fifteen percent (15%) above the standard subscription rate to cover regional infrastructure costs. When India-region hosting is activated, all Customer Data and personal data of candidates or employees located in India will be stored and processed exclusively within AWS Mumbai facilities. International transfers occur only where legally required for sub-processor services such as AI model API calls, and only with the Customer's explicit consent.

**(4)** The Provider actively monitors DPDP Act regulatory guidance and will adjust data storage locations as required by Indian law. If new data localization mandates require infrastructure changes, the Provider will notify affected customers at least ninety (90) days before implementation. Customers may terminate without penalty if mandated changes fundamentally alter service delivery or significantly increase costs.

**Art. 64 - Data Breach Notification Obligations**

**(1)** The Provider will notify affected Customers within seventy-two hours of discovering any data breach that compromises Customer Data security or confidentiality. Notification includes a description of the breach, categories of data affected, likely consequences, and measures the Provider is taking to address the breach and prevent recurrence.

**(2)** Customers remain responsible for complying with their own breach notification obligations to data subjects, regulatory authorities, and other third parties as required by applicable law. The Provider's notification to the Customer does not discharge the Customer's independent legal obligations regarding breach disclosure.

## Section IX -Compliance & Jurisdictional Requirements (Final ToS Version)

### Art. 65 -Customer Responsibility for Legal Compliance

**(1)** Customers must comply with all applicable employment, anti-discrimination, and labor laws in the jurisdictions in which they operate and where candidates or employees are located. This is an independent obligation of the Customer from its use of the Platform, and cannot be delegated to the Provider.

**(2)** While the Platform supports HR processes, it does not ensure legal compliance. Customers remain solely responsible for ensuring that their employment practices, hiring decisions, and use of AI-assisted outputs comply with applicable law.

### Art. 66 -U.S. Employment Law Compliance

**(1)** Customers who operate in the United States are required to comply with federal employment laws, such as Title VII of the Civil Rights Act; the Americans with Disabilities Act; the Age Discrimination in Employment Act; and the Equal Pay Act. Recommendations generated by AI should not be used in a way that facilitates discrimination against people based on a protected characteristic.

**(2)** Customers must comply with relevant guidance from the EEOC regarding the use of AI and other automated processes in making employment decisions, including conducting adverse impact analyses where legally required.

**(3)** When the Platform outputs contribute to background-check-related decisions, Customers will be obliged to follow the Fair Credit Reporting Act requirements on disclosure, candidate authorizations, and adverse action procedures.

**(4)** Customers operating in New York City are required to comply with Local Law 144 relating to bias audits of automated employment decision tools and required notifications to candidates. Customers operating in California are required to comply with the CCPA/CPRA, including disclosure obligations related to automated decision making.

### Art. 67 - Compliance with India DPDP Act

**(1)** Customers operating in India or processing personal data of individuals located in India shall be subject to the Digital Personal Data Protection Act, 2023. Explicit, informed, and freely given consent shall be required before uploading personal data to the Platform.

**(2)** Consent shall be given through explicit affirmative action. Data principals must be informed about the exact purposes of the processing, including the use of AI for analysis.

**(3)** Where required, Customers shall provide mechanisms for data principals to withdraw consent at any time, and upon withdrawal, Customers shall delete the individual's data from the Platform or rely on an alternative lawful basis.

**(4)** Where the processing of personal data of individuals under eighteen years of age is involved, Customers shall obtain verifiable parental or guardian consent. The Platform is not designed to process children's data, and such use should be avoided unless strictly necessary and in full compliance with the requirements under DPDP.

**(5)** Indian customers shall maintain a designated point of contact for data principal grievances and respond within statutory timelines. Customer responsibilities for candidate data grievances remain separate from those handled by the provider.

**Art. 68 - Candidate and Employee Notification Requirements**

**(1)** When using the Platform to process candidate applications or employee information for employment purposes, the Customer must notify affected individuals that AI assists in analyzing their data. This requirement applies under GDPR Article 22, India DPDP Act, and US state laws including NYC Local Law 144. Notification must occur at or before data collection.

**(2)** For New York City positions, the Customer must provide notification at least ten days before using AI to screen applications. For GDPR-covered candidates, notification must occur when applications are submitted. For candidates in India, notification must be in clear language with explicit consent obtained specifically for AI processing.

**(3)** At minimum, candidate notifications must include a clear statement that AI technology assists in reviewing applications or evaluating candidates, a description of what data the AI analyzes including resume content, work history, skills, and qualifications, an explanation that AI generates ranked candidate lists or recommendation scores that inform human decisions, confirmation that qualified human decision-makers review all AI recommendations before making employment choices, and contact information where candidates can ask questions or request human-only review.

**(4)** For candidates in New York City, notifications must additionally include the job qualifications and characteristics the AI considers, a summary of the data sources used for AI training, information about the most recent bias audit including the date conducted and results summary, and instructions for candidates to request an

alternative selection process or accommodation. For GDPR-covered candidates in the European Union, notifications must explain the logic involved in AI processing, the significance and envisaged consequences of such processing, and the candidate's right to obtain human intervention and contest automated decisions.

**(5)** For candidates in India subject to the DPDP Act, notifications must be provided in clear language in English and Hindi or the appropriate regional language. The notification must specify all categories of personal data collected, explain how AI will process that data for employment purposes, inform candidates of their right to access their data and request corrections, and explain how to withdraw consent for AI processing at any time. Withdrawal of consent must be as easy as giving consent initially.

**(6)** When candidates request human-only review, the Customer must flag those records in the Platform. Flagged candidates are excluded from AI processing and accessible only for manual review. Qualified personnel must conduct thorough human review without relying on AI recommendations.

**(7)** Compliance with candidate notification laws is exclusively the Customer's responsibility as the employer and data controller. The Provider supplies tools and guidance but cannot ensure Customer compliance. Per Art. 77, the Customer indemnifies the Provider against claims arising from inadequate candidate notifications.

### Art. 69 - Regulatory Changes

**(1)** If new legislation or government regulations compel the Provider to change the Platform or temporarily cease maintaining particular components of it, he will make such changes provided a reasonable amount of notice is given.

**(2)** If a regulatory change makes the Customer's primary use of the Platform illegal, then the Customer is entitled to terminate the subscription without penalty. No refunds are made for periods before termination unless legally required.

### Art. 70 - Industry-Specific Limitations

The Platform is not designed or certified to process industry-specific regulated data, such as protected health information under HIPAA or financial regulatory data. Customers are solely responsible for compliance with any laws or regulations applicable to their business.

## Section X -WARRANTIES, LIABILITY & INDEMNIFICATION

### Art. 71 - Limited Warranties

**(1)** Provider hereby warrants that it holds the legal right to supply the Platform and grant the licenses set out in these Terms. Provider warrants that the Platform shall substantially comply in all material respects with the Service Level Agreement during the Subscription Period.

**(2)** Each Customer warrants that he or she is authorized to upload the Customer Data onto the Platform and process personal data of candidates and employees by means of the Service. Each Customer also warrants that he or she uses the Platform in compliance with local employment laws.

**Art. 72 -Disclaimers and AI-Specific Limitations**

**(1)** Notwithstanding the limited warranties in Article 71, the Platform is made available to you on an “as is” and “as available” basis without any warranty of any kind. Provider hereby disclaims all implied warranties to include the warranties of merchantability, fitness for specific purpose, and non-infringement.

**(2)** By their very nature, the output of the AI is probabilistic in form and may contain errors, inaccuracies, biases, or outdated data. To the fullest extent of the applicable law, the Provider expressly disclaims any warranty that the Recommendations are free from errors, unbiased, legal-compliant, and appropriate for any specific employment decision.

**(3)** Provider disclaims all warranties related to the accuracy, completeness, and validity of any AI-produced output for job descriptions, candidate assessments, policy documents, or employment recommendations. Customers are obligated to verify all AI-produced output prior to its implementation.

**(4)** The Provider does not provide for the functionality of the Platform free from interruptions or errors. Such interruptions may occur due to maintenance work, system breakdowns, third-party supplier failures, or other unavoidable situations.

**Art. 73 - Limitation of Liability**

**(1)** In all cases arising from the use of the terms of service and the platform, the Provider's cumulative liability to the Customer is limited to the amount paid by the Customer to the Provider in the previous three months prior to the occurrence of the event giving rise to the claim.

**(2)** In no circumstances shall provider be liable for any indirect, incidental, consequential, special, or punitive damages. Such damages include damages for lost profits, lost revenues, lost data, lost business opportunities, reputation damage, or the cost of obtaining substitute services.

**(3)** Provider expressly disclaims liability for employment-related claims of discrimination, wrongful termination suits, fines from regulatory agencies, complaints from job candidates, and any other third-party claims related to the use of the AI Output or the customer's use of the Platform in making employment-related decisions.

**(4)** These liability limits shall also apply if the Provider has been notified of the possibility of such damages occurring. Also, the limits shall apply if the remedy fails in its essential purpose.

**(5)** Nothing in these terms shall affect any liability for death or personal injury resulting from negligence, fraud, fraudulent representation, or any other liability that cannot by law be excluded or limited.

**Art. 74 -Customer Indemnification Obligation**

**(1)** The Customer shall indemnify, defend, and hold the Provider harmless from all claims, damages, losses, and expenses (including reasonable attorney's fees) in any way connected to the Customer's use of the Platform in violation of the terms of this agreement and the applicable law.

**(2)** Indemnification particularly includes the consequences of the Customer's employment-related conduct, such as discrimination suits, wrongful termination suits, violation of wage and hour laws, or other employment disputes in which the Customer relies on the output of AI systems in the absence of human review.

**(3)** Customer indemnifies Provider for any claim about its Customer Data, including but not limited to allegations of infringing the intellectual property rights of third parties, violation of privacy laws, defamatory statements, and unlawful gathering and processing.

**(4)** Any claim subject to indemnity shall be brought to the immediate notice of the Provider to the Customer. However, the Customer retains the right to conduct all litigation proceedings related to the claim. Nevertheless, the Provider is accorded the right to participate in the claim proceedings through its attorney. Additionally, the Customer shall not enter into any agreement in relation to the claim that admits the Provider's liability without seeking prior consent from the Provider.

**Art. 75 - Provider Indemnification Obligations**

**(1)** Provider agrees to indemnify Customer against third-party claims for the use of the Platform that allegedly infringes the patent, copyright, trademark, or trade secret of a third party. Such claim must occur within the scope of the Customer's authorized use of the Platform in compliance with these Terms.

**(2)** The foregoing indemnity obligation does not apply to a claim directed against the Customer in respect of the Customer Data, the Customer's interfacing of the Services with third-party systems, the Customer's altering of the capabilities of the Services, or the Customer's continued usage of the infringing functionality despite notice from the Provider to stop.

**(3)** If the Platform becomes or is likely to become the subject of an infringement suit, the Provider may either secure the Customer the right to continued use of the Platform, develop a different Platform having substantially equivalent functionality that avoids the allegedly infringing material, or discontinue the relevant functionalities with a pro-rated refund.

### Art. 76 -Indemnification Procedures

**(1)** There must be a timely written notice of the claim by the party seeking indemnification. Failure to give timely notice precludes indemnification only if it materially impinges on the ability to defend.

**(2)** Only the indemnifying party retains the right to control the defense of the claim for which indemnification is sought. However, the indemnified party may also participate in the defense of the claim through its counsel.

**(3)** Each indemnified party shall cooperate in the defense of the claim. Each indemnified party shall make its employees and documents available if needed. Each indemnified party's reasonable out-of-pocket expenses in cooperating in the defense of the claim will be reimbursed by the indemnifying party.

## Section XI -Support, SLA & Dispute Resolution

### Art. 77 -Technical Support and Response Times

**(1)** The Provider is available for technical support through email response, the support ticket system, and through messages within the platform. Business hours are Monday through Friday from 9:00 AM to 6:00 PM Eastern Time, excluding federal holidays in the U.S.

**(2)** Response times for support levels depend on the support plan chosen. Standard plan users get their responses within forty-eight business hours. Professional plan users get their responses within twenty-four business hours. Enterprise plan customers get their responses within four business hours for critical issues related to access on the platform.

**(3)** Support includes the functionality of the Platform, administration of accounts, billing inquiries, and problem resolution for the Platform's functionality. However, the Platform's support excludes the areas of consulting work, software customization for

the Platform's functionality, employment law-related consultation, or Customer's in-house HR procedures.

**Art. 78 - Service Level Commitments and Remedies**

**(1)** The Provider also agrees to ensure the Platform's uptime of at least 98.9% every month, excluding the scheduled maintenance windows and the force majeure instances. Scheduled maintenance will take place within the announced time windows on weekends at least seventy-two hours in advance.

**(2)** Customers who are impacted by Platform availability being below the committed levels in any given month because the Provider system failed may seek service credits. Customers may earn 5% per percentage point below the committed threshold. However, the service credits earned do not go beyond 15% of the customer's monthly fee.

**(3)** Service credit must be requested within thirty days of the month of the outage. Credits must specify the dates and times of the outage. Customers must provide proof of the outage. Approved credits will be credited to the Customer's next bill. Service credits are the Customers' sole remedy for availability-related outages. Credits do not provide for refunds in dollars.

**(4)** Downtime resulting from Customer actions, third-party service outages, internet-connectivity problems beyond the Provider's control, Distributed Denial of Service attacks, and other Force Majeure Events enumerated in Section XIII are not counted in the calculation of uptime in the SLA.

**Art. 79 - Governing Law and Jurisdiction**

**(1)** Terms for Business Customers and individual customers in the United States are governed by the laws of the State of Delaware without reference to the conflict-of-laws principles. Any and all disputes will be subject to the jurisdiction of the courts of the State of Delaware.

**(2)** Any individual customer in India who is considered a consumer within the framework of the Consumer Protection Act 2019 will be subject to the laws of India. Such customers are free to approach consumer dispute redressal forums within the jurisdiction of their residential areas despite the arbitration clause in the terms. For dispute resolution procedures and arbitration provisions, refer to Art. 83, which includes specific carve-outs for Indian consumer rights.

**(3)** Where the Customer is also a Business in India, the terms will be governed by Indian law. There shall be exclusive jurisdiction in the courts of Bangalore.

**Art. 80 - Dispute Resolution and Arbitration**

**(1)** Prior to the institution of formal proceedings, the parties must make good faith efforts to resolve the dispute through negotiation. Any party may initiate the process of negotiation by giving written notice of the dispute to the other party's representative. Parties must negotiate for at least thirty days prior to instituting arbitration proceedings.

**(2)** Failure of the parties to reach an agreement shall render all disputes arising from the contract subject to binding arbitration in accordance with the Commercial Arbitration Rules of the American Arbitration Association. Such arbitration shall be administered by one arbitrator in English. Each side shall bear its own expenses. However, the arbitrator may award reasonable attorney's fees to the winning side.

**(3)** The arbitration requirement does not apply in cases that may be brought in small claims court if the claim value is within the jurisdictional limits for such courts. Any of the parties may seek injunctive relief in court in the event of intellectual property theft, confidentiality breaches, data security breaches, or in cases requiring immediate court attention.

**(4)** Individual customers in India retain all rights afforded by the Consumer Protection Act 2019 to bring their grievances against the Provider before the consumer dispute redressal forums.

**(5)** Individual customers in California may opt out of arbitration by sending their written notice to the Provider within thirty days from the registration of their accounts.

**(6)** All parties hereby waived their rights to assert the claim in class actions, representative suits, or consolidated proceedings. Each claim must proceed on an individual basis. This class action waiver shall not apply in instances in which class action waivers are banned by mandatory consumer protection laws.

## Section XII -General Provisions

### Art. 81 -Notices and Communications

**(1)** All formal notices under these terms must be delivered in writing to be legally effective. Written notice includes email sent to the registered email address on file, messages delivered through the Platform's notification system, or physical mail sent via registered or certified post with return receipt requested.

**(2)** Notices to the Provider should be sent to the official contact address published on the Provider's website or to the legal notices email address specified in the Customer's account documentation. Notices to the Customer will be sent to the

email address associated with the Customer's account or, for Business Customers with enterprise agreements, to the notice address specified in the Order Form.

**(3)** Notices are deemed effectively delivered on the date of email transmission if sent during business hours, or on the next business day if sent after hours. Physical mail notices are effective five business days after posting for domestic delivery or ten business days for international delivery. Platform notification system messages are effective immediately upon posting to the Customer's dashboard.

**(4)** Customers must maintain current contact information in their account settings. The Provider bears no responsibility for failed delivery of notices sent to outdated addresses if the Customer failed to update their information.

**Art. 82 -Assignment and Transfer**

**(1)** Customers may not assign, transfer, or delegate rights or obligations under these terms without the Provider's prior written consent. Any attempted assignment without consent is void and constitutes a material breach.

**(2)** The Provider may assign these terms or transfer rights and obligations to any affiliate, subsidiary, successor entity, or acquirer in connection with a merger, acquisition, corporate reorganization, or sale of substantially all assets related to the Platform. The Provider will notify Customers of any such assignment at least thirty days before the transfer becomes effective.

**(3)** If the Provider assigns this Agreement to a new entity in compliance with this Article, the Provider will notify Customers at least thirty (30) days before the assignment becomes effective. If the assignment results in a material reduction in service delivery quality, support standards, or materially changes the applicable data handling practices, affected Customers may terminate their subscription within thirty (30) days of receiving such notice, and will receive a pro-rated refund of any prepaid fees covering the period after the effective termination date.

**Art. 83 -Severability and Survival**

If any provision of these terms is determined to be invalid, illegal, or unenforceable by a court of competent jurisdiction, that provision will be limited or eliminated to the minimum extent necessary while the remaining provisions continue in full force and effect. The parties will negotiate in good faith to replace any invalid provision with a valid provision that achieves the original intent as closely as possible.

**Art. 84 -Waiver**

**(1)** Failure by either party to enforce any right or provision in these terms does not constitute a waiver of that right or provision. Waiver of any breach does not waive subsequent breaches of the same or different provisions.

**(2)** Any waiver must be in writing and signed by an authorized representative of the party granting the waiver to be effective. Oral waivers, course of dealing, or patterns of non-enforcement do not create binding waivers.

**Art. 85 -Entire Agreement and Amendments**

**(1)** These Terms & Conditions, together with all incorporated documents including the Privacy Policy, Data Processing Addendum, AI Transparency & Use Policy, Service Level Agreement, and Acceptable Use Policy, constitute the entire agreement between the parties regarding the subject matter herein. These terms supersede all prior or contemporaneous negotiations, discussions, agreements, understandings, and representations whether written or oral.

**(2)** The Provider may amend these terms by providing notice through email or Platform notification at least thirty days before the amendment effective date. Continued use of the Platform after the effective date constitutes acceptance of the amended terms.

**(3)** If the Customer does not accept material amendments that substantially alter the nature of the service or significantly restrict Customer rights, the Customer may terminate the subscription before the amendment effective date and receive a pro-rated refund for unused prepaid periods.

**(4)** No modification, amendment, or waiver of these terms by the Customer is binding unless agreed to in writing by an authorized representative of the Provider.

**Art. 86 -Force Majeure**

**(1)** Neither party is liable for failure or delay in performance caused by circumstances beyond its reasonable control. Force majeure events include natural disasters, acts of war or terrorism, government actions or restrictions, epidemics or pandemics, utility failures, internet backbone disruptions, labor disputes not involving the party's own employees, and other unforeseeable events that prevent performance despite reasonable efforts.

**(2)** Outages or degradations of third-party AI providers beyond both parties' reasonable control are treated as force majeure and do not constitute SLA breaches. Current providers include OpenAI, Anthropic, and AWS. Force majeure protection applies only to complete outages under forty-eight hours, degradations under seven days, and outages caused by government mandates or legal restrictions.

**(3)** The following are not protected by force majeure and are treated as Provider service failures subject to SLA remedies. Recurring outages exceeding three incidents of two-plus hours within thirty days, prolonged degradations exceeding seven days, the Provider's failure to use available backup providers during extended outages, and known reliability issues the Provider failed to address.

**(4)** The Provider evaluates AI provider reliability continuously and maintains relationships with multiple providers to enable failover during outages. Backup providers may result in temporary differences in output quality or processing speed. If force majeure conditions persist beyond thirty consecutive days, either party may terminate with written notice and the Customer receives pro-rated refunds for unused prepaid periods.

**Art. 87 -Independent Contractors**

Nothing in these terms creates a partnership, joint venture, agency, franchise, employment, or fiduciary relationship between the parties. The Provider and Customer are independent contractors. Neither party has authority to bind the other or to incur obligations on the other's behalf without prior written authorization.

**Art. 88 -No Third-Party Beneficiaries**

These terms are for the exclusive benefit of the Provider and Customer. No third party, including candidates whose information is processed through the Platform, employees, contractors, or other individuals, has any right to enforce or benefit from any provision of these terms.

**Art. 89 -Language and Interpretation**

**(1)** The authoritative version of these terms is the English language version. Translations provided for convenience have no legal effect if they conflict with the English text.

**(2)** Section headings and article titles are for reference only and do not affect interpretation. Use of "including" or "such as" is illustrative and not limiting unless explicitly stated as exhaustive.

**Art. 90 -Survival**

Provisions that by their nature should survive termination remain in effect after these terms end. Surviving provisions include intellectual property rights, confidentiality obligations, payment obligations for services already rendered, warranty disclaimers, liability limitations, indemnification duties, dispute resolution procedures, and these general provisions.

**Art. 91 -Compliance with Laws**

Both parties agree to comply with all applicable laws, regulations, and industry standards in performing their respective obligations under these terms. This includes compliance with export controls, sanctions, anti-corruption laws, data protection regulations, employment laws, and tax obligations in all relevant jurisdictions.

**Art. 92 -Counterparts and Electronic Signatures**

These terms may be executed in counterparts, each of which constitutes an original and all of which together constitute one agreement. Electronic signatures, including acceptance indicated by clicking "I agree" buttons or similar mechanisms during Platform registration, have the same legal effect as handwritten signatures and are binding on the parties.