Privacy Policy

PeopleBotApp processes personal data to deliver an AI-powered HR and recruitment platform for businesses and individual users across multiple jurisdictions. This Privacy Policy explains what data we collect, how we use it, how we share it, and the rights that individuals have under applicable global privacy laws. We describe our dual role as both a data controller and a data processor, depending on how customers engage with the Platform. Our practices follow the principles of transparency, data minimization, purpose limitation, and strong security protections. We outline the use of artificial intelligence technologies and the safeguards that prevent AI from making fully automated employment decisions. The Policy also details our international transfer mechanisms, including Standard Contractual Clauses and Transfer Impact Assessments. Data retention periods, deletion procedures, and customer export rights are clearly defined to ensure full lifecycle governance. We explain the rights of data subjects under GDPR, CCPA/CPRA, India's DPDP Act, and other global regulations. Our commitments include strong security controls, strict vendor management, and a prohibition on selling personal data. By using PeopleBotApp, you acknowledge and agree to the data practices described in this Privacy Policy.

SECTION I – OVERVIEW OF PEOPLEBOTAPP

Art. 1. Scope and Coverage

(1) PeopleBotApp, Inc is an AI-based Human Resource Helping Tool Company. The firm has designed a Human Resource Assistant Platform for recruitment, screening of candidates, and generation of employment-related content by using AI Technology. As part of the Human Resource Assistant Platform, the Provider collects, uses, shares & protects Personal Data, which is the subject of this privacy policy. Each Person has their own Privacy Policy; however, regardless of their Subscription Tier, Place of Origination, or method of access to the PeopleBotApp, whether as a Business Client subscriber, Individual Subscriber, or Candidate through a Business Customer's account, the same Policy applies to them.

(2) The Provider is under the obligation to make sure its data practices are transparent and in compliance with all laws around privacy according to the General Data Protection Regulation; The Digital Personal Data Protection Act of 2023 (India); The California Consumer Privacy Act & The California Privacy Rights Act of 2023 as well as any other Data Protection Laws that apply to the Provider in any region that the Platform is operating. This Policy provides visibility to help you understand how Your Decisions regarding the sharing and use of your personal data with PeopleBotApp are made transparent.

(3) The relation of this Privacy Policy to the other Agreements as set forth. Terms and Conditions; AI Transparency & Use Policy; Cookie Policy;

Art. 2 - Data Controller and Processor Roles

(1) PeopleBotApp, Inc. is a Delaware corporation. To the extent the Provider collects personal data directly from individual users and business customers in connection with account registration, billing, and use of the Platform, the Provider is the controller or fiduciary of such data under applicable law. By this, it is meant that the Provider determines the purposes and means of processing such data and bears primary responsibility for compliance with applicable privacy regulations concerning this information.

(2) With respect to candidate and employee personal data that business customers upload to the Platform for recruitment, screening, or other human resources purposes, the relationship is fundamentally different. In those circumstances, the business customer is the data controller or data fiduciary because the customer decides what candidate information to collect, what purposes to pursue with AI-assisted analysis, and how to use the resulting insights. The Provider is a data processor or data fiduciary on behalf of the customer, processing personal data only as instructed by the customer and within the parameters of the contracted service.

(3) This dual-role structure has important practical implications. Individual users and business account administrators should direct privacy inquiries about their own account information to the Provider using the contact details in Art. 39. Candidates and employees whose information appears in the Platform because a business customer uploaded it for recruitment or HR purposes should direct privacy requests to that business customer in the first instance, as the customer controls the personal data and must fulfill data subject rights. The Provider will cooperate with business customers to facilitate such requests where technically feasible and consistent with the Data Processing Addendum.

(4) For some processing activities, the Provider and business customers will be joint controllers pursuant to applicable law. This is the case when both parties play an active role in determining processing purposes and means, for example, configuring AI recommendation algorithms or defining data retention policies. Where joint controllership applies, the respective responsibilities of each party are specified in the Data Processing Addendum provided to business customers either upon account creation or, upon request, via the account dashboard.

Art. 3 - Key Definitions

1. **Personal data -** any information relating to an identified or identifiable natural person. This includes obvious identifiers such as names, email addresses, and identification numbers, as well as information that can be linked to identify someone when combined with other data. In the context of

the Platform, personal data includes account credentials, billing information, candidate resumes, employee records, and usage patterns that can be associated with specific individuals. The definition encompasses both data provided directly to the Platform and information generated through Platform use.

2. **Processing -** any operation performed on personal data, whether automated or manual. Processing includes collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, transmission, alignment, restriction, erasure, and destruction of personal data. When customers upload candidate information, analyze it using AI features, export results, or delete records, each of these activities constitutes processing. The Provider processes personal data throughout the service delivery lifecycle, from initial account creation through final data deletion after subscription termination.
3. **AI provider -** third-party artificial intelligence technology companies whose models power the Platform's recommendation engine and content generation features. Current AI providers include OpenAI and Anthropic, though this list may change as technology evolves. These providers receive certain user inputs and prompts to generate recommendations but operate under strict contractual limitations regarding data use and retention. Specific AI provider data handling practices are detailed in Art. 13 and the AI Transparency & Use Policy.
4. **HR data -** all employment-related personal information processed through the Platform. This category includes candidate applications and resumes, interview notes and assessments, job descriptions and requirements, performance evaluations, compensation information, and any other data relevant to recruitment, hiring, employee management, or workforce planning. Because HR data often reveals sensitive characteristics protected under employment and anti-discrimination laws, the Provider implements heightened security measures and processing restrictions for this data category.
5. **Candidate data -** refers to personal information concerning individuals who apply for positions or whose information is uploaded to the Platform for recruitment evaluation purposes. Candidate data typically includes contact details, work history, educational background, skills assessments, and any information derived from AI analysis of application materials. Candidates do not have direct accounts on the Platform but possess privacy rights under applicable laws, which they exercise through the business customers who control their data or by contacting the Provider as described in Art. 32 and Art. 33.
6. **The terms controller and processor** - specific legal meanings under data protection laws. A controller determines the purposes for which and the manner in which personal data is processed. A processor processes personal data on behalf of and according to the instructions of a controller. Under the Digital Personal Data Protection Act 2023 of India, equivalent terms are data fiduciary for controller and data processor for processor. Throughout this policy, these terms are used interchangeably to reflect their functional equivalence across different regulatory frameworks.

7. **Sensitive personal data** - refers to information that reveals or relates to particularly private aspects of an individual's identity or circumstances. This includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification purposes, health information, and data concerning sex life or sexual orientation. The Platform is not designed to collect or process sensitive personal data categories. Business customers must not upload such information unless absolutely necessary for legitimate employment purposes and only where permitted by applicable law with appropriate safeguards.
8. **Automated decision-making -** means using technology to make decisions about individuals without meaningful human involvement. Under regulations including the General Data Protection Regulation Article 22 and the Digital Personal Data Protection Act, individuals have special protections against solely automated decisions that produce legal effects or similarly significant impacts. The Platform is designed as a recommendation engine where AI generates suggestions and insights, but human decision-makers must review these recommendations before taking employment actions. This distinction is fundamental to the Platform's design and legal compliance framework.
9. **Third-party integrations** - external software applications and services that customers may connect to the Platform through official integration features. Common examples include applicant tracking systems, human resources information systems, communication platforms such as Slack or Microsoft Teams, calendar applications, and productivity tools. When customers authorize integrations, certain personal data may flow between the Platform and integrated services to enable requested functionality. Each integration operates under the third party's own privacy policy, though the Provider conducts security assessments before enabling integration partnerships.
10. **Cookies and tracking technologies** - small data files and similar mechanisms that collect information about Platform usage and user preferences. Cookies may be placed by the Provider or by third-party services integrated into the Platform. These technologies serve various purposes including maintaining login sessions, remembering user preferences, analyzing Platform performance, and supporting security features. Detailed information about specific cookies used, their purposes, and how to control them appears in the separate Cookie Notice accessible through the Platform footer and account settings.

SECTION II - WHAT DATA WE COLLECT

Art. 4 - Customer Account Information

(1) To create a Platform account, individuals and organizations must provide essential identifying details. Individuals need to submit their full name, a working email address, and choose a secure password. For business accounts, organizations must provide the company name, primary contact person, corporate email domain, and the country of operation.

(2) Payment details become necessary once customers move beyond trial periods or select paid subscription tiers. The Provider collects credit card numbers, expiration dates, security codes, and billing addresses through secure payment gateways. Bank account details may be provided instead for direct debit arrangements. Tax identification numbers are gathered from business customers in jurisdictions requiring documentation for invoicing- particularly in India where GST registration numbers must appear on compliant invoices.

(3) Customers configure accounts according to their operational demands and choices. Business subscribers designate which team members receive administrator privileges versus standard user access. Notification settings let people choose whether they want immediate alerts, daily digests, or minimal interruptions. Regional hosting preferences matter for customers subject to data localization requirements. Integration toggles control which external systems can exchange data with the Platform.

(4) Support interactions generate records that help resolve technical problems and track service quality. When someone opens a support ticket, the system captures the issue description, relevant screenshots, correspondence between the customer and support staff, and the ultimate resolution. Phone call logs note conversation dates and general topics discussed, though detailed recordings require explicit consent in jurisdictions mandating such protections. These records become essential when disputes arise about service delivery or when similar technical issues surface later.

Art. 5 - Candidate and Employee Data (Processed for Customers)

(1) Business customers determine what candidate information enters the Platform. Most upload standard application materials, including resumes, cover letters, and portfolios, but some include interview assessments, reference check notes, skills test results, or background verification reports. The variety reflects different hiring practices across industries and company sizes. A tech startup might focus heavily on coding challenge results, while a healthcare provider focuses on licensing verification and credential authenticity.

(2) AI analysis transforms raw application documents into structured insights by parsing resumes to identify key elements such as job titles, employment dates, educational institutions, and technical skills. This process allows the system to match candidate qualifications against job requirements, generating compatibility scores and showcasing relevant experience, thereby streamlining the hiring process and aiding managers in making data-driven choices. Interview question suggestions emerge based on gaps the AI detects between candidate background and role expectations. These derived insights do not replace human judgment; they organize information so hiring managers can make better-informed decisions more efficiently.

(3) Sensitive information sometimes appears in candidate materials despite recommendations against including it. A resume might show a graduation year that reveals an approximate age. Home addresses can signal a person's national origin or current immigration status. Career gaps explained through medical leave or parental responsibilities can touch on a person's health and family situation. The Platform does not extract this sensitive data for separate processing or model training. Business customers must evaluate whether such information should influence their hiring decisions under varying anti-discrimination laws.

(4) The distinction between controller and processor becomes critical with candidate data. Business customers act as controllers- they decide what information to collect, what analysis to request, and how results inform hiring choices. The Provider acts as their processor, handling data solely according to the customer instructions embedded in how they use Platform features. This arrangement means candidates exercise their privacy rights primarily through the employers or recruiters who uploaded their information.

(5) System-generated metadata tracks how candidate information moves through the Platform. Timestamps show when resumes were uploaded, who accessed each profile, what AI analyses were requested, and when records were modified or deleted. This audit trail serves multiple purposes: it helps customers demonstrate compliance with fair hiring practices, assists in troubleshooting technical issues, and provides evidence if disputes arise about how candidate data was handled.

Art. 6 - Technical and Usage Data

(1) Every interaction with the Platform leaves technical traces in server logs. These logs record details such as the IP addresses where connections originate, the types of browsers people use, whether they’re on a phone or computer, and how they move through the site- showing which features get the most use.

(2) Performance monitoring proactively identifies issues before users experience them by tracking page load times, API call success rates, memory and processing power usage, and system bottlenecks. For instance, if page load times increase, the system alerts engineers to optimize resources, ensuring a seamless user experience. When response times creep upward or error rates spike, engineering teams investigate before widespread service degradation occurs. This data also guides infrastructure scaling decisions; if customer growth concentrates in Asian time zones, server capacity is expanded accordingly.

(3) Aggregate analytics inform product strategy without tracking individuals. The Provider observes that certain AI features get heavy usage while others gather dust, particular subscription tiers attract specific customer segments, integration partnerships drive adoption or create support burdens, and feature combinations predict customer retention or churn. These patterns influence which capabilities receive development resources, what pricing changes might make sense, and where user experience improvements could yield a significant impact.

(4) Security systems are designed to continuously monitor and protect against threats. For example, if multiple failed login attempts occur, the system implements progressive delays to thwart brute force attacks. Additionally, if an account shows activity from distant locations within a short timeframe, it flags this as impossible travel, prompting further verification.

(5) Password reset requests from unrecognized devices prompt additional verification steps. This monitoring operates continuously in the background, intervening only when suspicious patterns emerge.

Art. 7 - Data from third-party integrations

(1) Through its functionalities, the platform allows customers to connect to third-party tools that they already use. Each integration requires explicit permission, specifying what data the external service has access to and what information is returned to the Platform.

(2) Data exchange varies depending on the purpose of the integration and the customer's configuration. Synchronization with an applicant tracking system can copy applicant profiles in both directions, keeping the information up to date. Customers grant these permissions through integration setup wizards that explain exactly what data each connection will have access to.

(3) Third-party services operate outside the Provider's control once data leaves the system. The Provider evaluates integration partners before activating connections by reviewing their security certifications and contractual data protection commitments. However, customers bear the ultimate responsibility for understanding what happens to their data once they authorize its transfer to external systems.

SECTION III - HOW WE USE YOUR DATA

Art. 8 - Provision of services and operation of the platform

(1) Creating and maintaining accounts requires processing the registration information provided by customers. The system verifies login attempts by comparing the entered access data with the stored account data. The subscription level determines which features and to what extent each user has access.

(2) The basic functionality depends on continuous data processing as customers use different features of the platform. Uploading a candidate's resume triggers analysis algorithms that extract structured information. Searching for candidates who meet certain criteria makes queries to databases created from previously uploaded profiles. The AI analysis request sends the relevant data to language models that generate recommendations. The system must store this information to provide results, including allowing for subsequent improvements and preserving the results of the work for future reference.

(3) Personalization makes the platform more effective for regular users. The interface remembers the preferred language, the way the candidate lists are sorted, the

widgets on the dashboard that are most useful to the user, and the candidates they have recently viewed.

(4) Operational messages inform customers about issues affecting their accounts. Subscription renewal reminders arrive before billing dates. Notifications of failed payments explain why service may be interrupted if payment issues are not resolved. Security alerts flag suspicious login attempts or unusual activity patterns. Maintenance notifications warn of planned service outages.

Art. 9 - Artificial intelligence processing and recommendations

(1) Language models differ in their interpretation of unstructured text, which varies significantly in format and content. AI extracts relevant qualifications from each format by identifying job titles, skills, length of experience, and educational qualifications, despite differences in presentation. This interpretation creates consistent data fields that allow meaningful comparisons between candidates.

(2) Matching algorithms assess how well candidates' qualifications match the requirements for the position. The analysis considers obvious factors such as required experience and specific technical skills, but also uncovers finer patterns such as consistency in career progression, relevance of industry experience, and combinations of skills that suggest adaptability. The results are presented as numerical scores, explanatory summaries, and comparisons that highlight why certain candidates are ranked higher than others. These assessments support human decision-making, rather than replacing it.

(3) Some administrative tasks lend themselves to automation without entering the realm of autonomous decision-making. Substantive judgments about candidate quality, progression to interviews, hiring decisions, or rejection notifications require direct human action and are not performed automatically.

Art. 10 - Customer Support and Communications

(1) Effective technical support requires understanding what customers have experienced before problems arise. Support staff have access to review account activity, check error logs showing what went wrong, and check browser and network configurations that may contribute to problems.

(2) Product updates and policy changes reach customers through multiple channels. Significant feature changes require detailed emails explaining the new capabilities and how to access them. Substantial changes to privacy practices, security measures, or contractual terms receive advance notice- typically a minimum of thirty days- allowing customers to review the changes and decide whether continued use of the platform remains acceptable under the changed terms.

Art. 11 - Analytics, security, and improvements

(1) Product development decisions shall be based on an analysis of the collective use of the platform by customers. Feature adoption metrics reveal which features add value and which confuse users or go unnoticed.

(2) Threat detection systems operate continuously, monitoring patterns that indicate security risks or violations of the Terms and Conditions. Attempts to fill out credentials generate distinctive patterns- multiple failed logins to many accounts in short periods of time. Data scraping manifests as unusually high volumes of API requests or systematic profile browsing that no human could do manually. Malicious software uploaded to candidates' resumes is detected by file scanning before it reaches the computers of hiring managers. When these detection systems are triggered, responses range from temporary throttling to account suspension to investigation completion, depending on the severity of the threat.

(3) Service improvements balance customer feedback, technical performance data, and strategic priorities. Customer suggestions submitted through feedback channels sometimes inspire new opportunities or reveal unmet needs.

Art. 12 - Legal Compliance and Security

(1) Operating in multiple jurisdictions creates complex compliance obligations that require careful documentation and process implementation. Tax authorities require documentation of transactions supporting reported revenue. Data protection regulators may require evidence demonstrating lawful grounds for processing and consent mechanisms. The provider maintains these records not only because it is required by regulation, but also because they demonstrate responsible business practices and protect customers who encounter similar documentation requests.

SECTION IV - PROCESSING SPECIFIC TO ARTIFICIAL INTELLIGENCE

Art. 13 - Partnerships with artificial intelligence providers and data sharing

(1) The Provider processes personal data through artificial intelligence models provided by third-party technology companies, in particular OpenAI, Inc. and Anthropic PBC, which are AI subcontractors under the applicable data protection provisions. These AI providers receive limited categories of data solely for the purpose of generating recommendations, content suggestions, and analytical results requested by business customers through the Platform's features.

(2) The data transferred to AI providers consists exclusively of text input data submitted by authorized users, including candidate resume content, job descriptions, interview questions, and other documents related to hiring. The Provider does not transmit personally identifiable metadata, user account access data, payment information, or technical usage logs to AI providers unless such information is contained in the text content uploaded by the customers themselves.

(3) The provider maintains contractual agreements with each AI provider imposing the following mandatory restrictions:

1. Prohibition on the use of transferred data for training, improving, or developing AI models, unless explicit consent has been obtained from the business customer through account settings;
2. Requirement to process data solely for the purpose of generating the requested results and to delete or anonymize all submitted content within the maximum period specified in the data retention policy of the relevant AI provider;
3. Implementation of encryption protocols that meet industry standards for data in transit between the Platform and the systems of AI providers;
4. Compliance with applicable data protection regulations in the jurisdictions in which the platform operates, including the GDPR, the Indian DPDP Act 2023, and US state privacy laws.

(4) The Provider does not control and is not responsible for the processing by AI providers that is performed outside the contractual parameters specified in paragraph (3). Business customers acknowledge that AI providers operate under their own privacy policies and terms of use, which customers should review independently before authorizing the processing of candidate or employee data by AI.

(5) Current AI providers and their relevant data processing documentation are published at https://www.peoplebotapp.com/ai-usage and updated within 30 days when new AI providers are added or existing providers are replaced. Business customers shall receive email notification of material changes to agreements with AI providers at least 15 days prior to their implementation.

Art. 14 - Anonymization and data minimization

(1) The provider shall apply the principles of data minimization to all AI processing operations, transmitting only the specific text content necessary to generate the requested results. Metadata, user identifiers, account information, and technical details shall be systematically excluded from transmission to AI providers.

(2) Anonymization techniques shall be applied prior to certain AI processing operations, although complete anonymization is not always technically feasible given the nature of employment data, where the names of applicants, contact information, and identifying data are an integral part of resumes and application documents. Where anonymization would render the AI analysis meaningless or unusable, the Provider processes the data in pseudonymized form or with minimal identifiers.

(3) Business customers bear the primary responsibility for ensuring that uploaded candidate materials do not contain excessive amounts of personal data that are not related to job qualifications. The Provider recommends removing or editing sensitive information such as national identification numbers, passport details, financial account information, medical conditions, or family relationship details before uploading documents for AI analysis.

Art. 15 - Artificial Intelligence Training Data Policy

(1) The Provider unequivocally declares that customer data, candidate information, and employment-related content processed through the Platform shall not be used for training, improving, refining, or developing artificial intelligence models operated by the Provider or by artificial intelligence subcontractors, except in cases where business customers give their explicit consent through their account configuration settings.

(2) This prohibition applies regardless of whether the data is anonymized, aggregated, or otherwise modified. The Provider does not provide customer input data generated by artificial intelligence output data or any derivative data for training datasets, model improvement initiatives, or research projects conducted by artificial intelligence providers or third parties.

(3) The explicit consent mechanism for authorizing the use of data for artificial intelligence training works as follows:

1. By default, the configuration of all accounts prohibits the use of artificial intelligence training, Business customers can activate their consent through the account settings, where explicit warnings describe the consequences of allowing the use of training data;
2. Consent applies only to future data- data processed prior to activation remains excluded from training dataset. Customers can revoke consent at any time, with revocation taking effect within 72 hours;
3. Individual users who use the platform for personal purposes rather than business operations cannot activate the option to use data for AI training, as this option is available exclusively to business account administrators.

(4) There are some mandatory exceptions to the training prohibition when required by law or essential for the security of the service:

1. Anonymized, aggregated usage statistics showing the adoption rate of platform features, error rates, and performance metrics may be used to improve the stability and reliability of the service;
2. Security threat data, including malware samples, attack patterns, and abuse indicators discovered through artificial intelligence processing, may be shared with security research communities and artificial intelligence providers for the purpose of improving defenses;
3. Data necessary to comply with valid legal procedures, regulatory investigations, or court orders may be disclosed in accordance with legal requirements, although such disclosure does not constitute authorization for artificial intelligence training purposes.

Art. 16 - Ownership of artificial intelligence results and restrictions on use

(1) All intellectual property rights in content generated by AI through the platform's features are immediately and fully transferred to the business customer who requested such generation. This transfer covers job descriptions, candidate resumes, interview questions, evaluation rubrics, email templates, and any other text, analysis, or recommendations produced through AI processing.

(2) The transfer of intellectual property described in paragraph (1) remains subject to mandatory legal restrictions on the use of AI results in the context of employment:

1. Business customers may not use AI-generated recommendations as the sole basis for adverse employment decisions, including rejecting candidates, declining to interview, terminating employment, or determining compensation, without meaningful human review by qualified personnel;
2. AI results must not be used in a manner that facilitates unlawful discrimination based on protected characteristics under applicable employment laws, including race, color, religion, gender, national origin, age, disability, genetic information, or other classifications protected in the jurisdictions in which customers operate;
3. Business customers must implement human oversight procedures that comply with the requirements of Article 22 of the GDPR, Section 10 of the Indian DPDP Act, and applicable U.S. employment regulations before using AI results in hiring processes;
4. Content generated by artificial intelligence remains subject to the usage policies of major artificial intelligence providers, which prohibit certain applications, including but not limited to harassment, discrimination, generation of misinformation, and circumvention of employment verification requirements.

(3) The provider disclaims any warranty regarding the accuracy of the results of artificial intelligence, the absence of bias, compliance with regulatory requirements, or suitability for specific hiring decisions. Business customers assume full responsibility for verifying the results of artificial intelligence prior to implementation, conducting independent bias audits where required by law, and ensuring compliance with all applicable employment, anti-discrimination, and data protection.

(4) As a practical limitation: AI-generated content may unintentionally resemble existing copyrighted works or contain factual inaccuracies, despite the Provider's quality control efforts. Business customers must independently verify that AI results do not infringe on the intellectual property rights of third parties before publication, commercial use, or distribution outside of internal evaluation purposes.

(5) The ownership rights and usage restrictions set out in this Article should be read in conjunction with Article 35 (Automated decision-making and transparency of AI), which establishes the rights of applicants to object to AI processing and to request a review by humans only. Ownership rights over AI outputs do not override these individual rights and do not remove customers' obligations to respect them.

SECTION V - LEGAL BASIS FOR PROCESSING

Art. 17 - Legal Grounds for Data Processing

(1) The Provider processes personal data exclusively on the basis of lawful grounds established under Article 6 of Regulation (EU) 2016/679 (GDPR), Section 8 of the Digital Personal Data Protection Act 2023 (India), and corresponding provisions of applicable data protection legislation in jurisdictions where the Platform operates. Each processing activity rests on one or more of the legal bases enumerated in paragraphs (2) through (6) of this Article.

(2) Processing necessary for the performance of a contract constitutes the primary legal basis for the majority of Platform operations. This legal ground applies in the following circumstances:

1. Account creation and authentication processing, where the Provider must verify credentials and maintain login functionality to deliver contracted Platform access;
2. Subscription billing and payment processing, which cannot occur without processing payment method details, billing addresses, and transaction records;
3. Service delivery including AI processing of customer-uploaded data, feature provisioning according to subscription tier, and technical support provision;
4. Communication of service-related information essential to contract performance, including password reset confirmations, payment receipts, security alerts, and subscription status notifications.

(3) Where the Provider processes personal data of candidates and employees uploaded by business customers, the legal basis derives from the contractual relationship between the Provider and the business customer acting as data controller. The Provider processes such data as a processor on behalf of and according to instructions from the business customer, who must independently establish appropriate legal grounds under their own data protection obligations.

(4) Processing based on legitimate interests applies to specific Platform operations where processing serves interests of the Provider or third parties, provided such interests do not override the fundamental rights and freedoms of data subjects. Legitimate interest processing occurs in the following contexts:

1. Fraud prevention and security monitoring, including detection of unauthorized access attempts, identification of payment fraud patterns, and prevention of Terms & Conditions violations such as data scraping or competitive intelligence gathering;
2. Service improvement through analysis of aggregate usage patterns, error rate monitoring, performance optimization, and product development prioritization, conducted without creating individual user profiles for marketing purposes;

3. Network and information security measures protecting Platform infrastructure, customer data, and business operations from cyber threats, malware, distributed denial-of-service attacks, and other security incidents;
4. Internal administrative purposes including record-keeping for accounting obligations, maintenance of transaction histories for dispute resolution, and documentation supporting legal compliance demonstrations;
5. Direct marketing communications to existing customers regarding similar services, subject to customer right to object at any time through unsubscribe mechanisms provided in each communication.

(5) Processing based on consent applies when the Provider collects explicit, informed, and freely-given agreement from data subjects for specific processing activities. Consent serves as the legal basis for:

1. Marketing communications sent to individuals who are not existing customers or who receive promotions for services substantially different from those previously purchased;
2. Non-essential cookies and tracking technologies beyond those strictly necessary for Platform functionality, as detailed in the separate Cookie Notice;
3. Optional data sharing with third-party integration services where such sharing exceeds what is necessary for contracted service delivery;
4. Participation in optional surveys, feedback programs, beta testing initiatives, or research studies;
5. AI training data usage by business customers who activate opt-in authorization through account settings, as specified in Article 15(3).

(6) Consent obtained under paragraph (5) satisfies the following mandatory requirements:

1. Request for consent is presented in clearly distinguishable form, separate from other terms and conditions, using plain language intelligible to average data subjects;
2. Data subjects receive clear information about the specific processing purposes, data categories involved, identity of recipients, and their right to withdraw consent at any time;
3. Consent actions require affirmative opt-in through explicit actions such as clicking consent buttons or checking empty boxes, with pre-ticked boxes and inactivity not constituting valid consent;
4. Withdrawal mechanisms are as simple and accessible as the original consent process, with withdrawal taking effect immediately or within technically necessary processing periods not exceeding 72 hours;
5. Withdrawal of consent does not affect the lawfulness of processing conducted before withdrawal, nor does it impact processing based on alternative legal grounds such as contract performance or legitimate interests.

(7) Processing necessary for compliance with legal obligations applies in all cases where the storage or disclosure of data is mandatory under applicable law. This legal basis covers:

1. Retention of tax and accounting records as required by tax authorities in the jurisdiction, typically for a period of 5 to 7 years after the end of the financial year in which the transactions were carried out;
2. Responses to court orders, subpoenas, regulatory investigations, and requests from law enforcement authorities that meet the procedural requirements of applicable law;
3. Mandatory notification of supervisory authorities and affected data subjects of breaches, as required by Articles 33-34 of the GDPR, Section 6 of the Indian DPDP Act, and the relevant provisions of US state privacy laws;
4. Labor law documentation obligations imposed on business customers, where the Provider assists in maintaining audit trails and documentation supporting the demonstration of fair hiring practices.

(8) Processing related to tasks carried out in the public interest or in the exercise of official authority does not apply to the Provider's activities, as the Platform serves commercial purposes rather than public sector functions.

(9) For each processing activity, the Provider maintains internal documentation specifying the applicable legal basis, the specific purpose, the categories of data, the storage periods, and the categories of recipients. Business customers acting as data controllers for applicants and employees shall bear equivalent documentation obligations under their own data protection compliance frameworks.

(10) Where the Provider relies on legitimate interests as a legal basis pursuant to paragraph (4), data subjects have the right to object to such processing at any time on grounds relating to their particular situation.

(11) Changes to the legal basis for specific processing activities require an assessment of whether such changes necessitate obtaining new consent, providing additional notice to data subjects, or conducting data protection impact assessments. Substantial changes to the legal bases affecting existing data subjects give rise to notification obligations under the rules of Article 38 (Changes to this Privacy Policy

SECTION VI - DATA SHARING AND RECIPIENTS

Art. 18 - Service Providers and Subcontractors

(1) The Provider engages third-party service providers and subcontractors to provide the functionality of the Platform, maintain the infrastructure, process payments, and support business operations. These entities have access to personal data strictly limited to what is necessary to perform their designated functions and operate in accordance with privacy policies that ensure data protection standards equivalent to those set forth in this Privacy Policy.

(2) The categories of service providers and subcontractors currently engaged by the Provider include:

1. Cloud infrastructure providers hosting the Platform's systems and databases, in particular Amazon Web Services with primary data centers located in the US-East-1 and US-West-2 regions, with an option for hosting in India (AWS Mumbai ap-south-1), available to business customers subject to data localization requirements;
2. AI technology providers providing natural language processing and machine learning capabilities, specifically OpenAI, Inc. and Anthropic PBC, whose data processing practices are described in detail in Article 13;
3. Payment operators processing subscription accounts, credit card transactions, and financial payment transactions, operating under the Payment Industry Data Security Standards certification;
4. Email service providers that deliver transactional notifications, support communications, and authorized marketing communications to customers;
5. Customer support platforms that manage support ticketing systems, live chat functionality, and help center operations;
6. Security and monitoring services that provide threat detection, intrusion prevention, malware scanning, and vulnerability assessment capabilities;
7. Analytics providers that process aggregated usage data for the purpose of improving services, subject to data minimization and anonymization requirements.

(3) Each subcontractor has explicitly stated in its privacy policy that it is committed to the following contractual obligations:

1. Implementing appropriate technical and organizational security measures that meet the standards set out in Articles 26-28, including encryption, access control, and breach detection capabilities;
2. Maintaining the confidentiality of all personal data accessed during the provision of the service, with confidentiality obligations remaining in force even after the termination of the contract;
3. Assisting the Provider in responding to requests related to the rights of data subjects, conducting data protection impact assessments, and managing security incidents;
4. Deleting all personal data upon termination of the contract or at the request of the Supplier, except where their storage is required by applicable law;

(4) The Provider maintains an up-to-date list of all subcontractors that process personal data in this privacy policy and updated within 15 business days when subcontractors are added, replaced, or removed. Business customers shall receive email notification of anticipated changes to subcontractors at least 30 days before the new subcontractors begin processing personal data.

(5) Business customers may object to new subcontractors within 14 days of receiving the notification under paragraph (4). Valid objections based on documented data protection concerns lead to good-faith negotiations to resolve the issues, identify alternative subcontractors, or allow customers to terminate their subscription without penalty if resolution proves impossible.

Art. 19 - Business Transfers and Corporate Events

(1) The Provider reserves the right to transfer personal data in connection with mergers, acquisitions, corporate reorganizations, asset sales, insolvency proceedings, or other business transactions affecting the ownership or control of the Platform or the Provider's business operations.

(2) Before transferring the activity pursuant to paragraph (1), the Supplier must:

1. Perform due diligence to ensure that the acquirer or successor undertakes to comply with data protection standards that are no less stringent than those set out in this Privacy Policy;
2. Notify the data subjects concerned in advance of the intended transfer, specifying the successor and describing any material changes in data processing practices;
3. Provide data subjects with a minimum period of 30 days to exercise their applicable rights, including requests for data erasure, before the transfer takes effect;
4. Require the successor to comply with all data protection commitments, consent restrictions, and processing restrictions applicable to the transferred data.

(3) The notification of the transfer of the business pursuant to paragraph (2) shall be delivered by:

1. An email notice to all registered account holders;
2. A public announcement on the Provider's website;

(4) If the transferee in a transfer of business intends to process personal data for purposes incompatible with or different from the original purposes of collection, such processing requires obtaining new consent from the data subjects concerned or establishing alternative legal grounds pursuant to Article 17.

(5) Business transfers do not affect the rights of data subjects set out in Sections X, XI, and XII of this Privacy Policy. Data subjects retain their full rights of access, rectification, erasure, restriction, portability, objection, and complaint with regard to their personal data, regardless of changes in ownership affecting the Provider.

(6) The rules of this article shall also apply in the event of a sale of company shares exceeding 50% of the total capital of the company.

Art. 20 - Legal Requirements and Law Enforcement

(1) The Provider shall have the right, without prior notice, to disclose personal data to government authorities, law enforcement agencies, regulatory authorities, or judicial authorities when required by legal process or applicable law. Such disclosures shall only be made after verification that the requests comply with procedural requirements and fall within the lawful jurisdiction of the requesting authority.

(2) The provider shall notify the data subjects concerned of the disclosure of data within 72 hours, unless:

1. Notification is prohibited by law, court order, law enforcement directive, or legal provision;
2. Notification would impede ongoing investigations or create risks to public safety;
3. Legal process expressly prohibits disclosure of the existence of the request;
4. Notification proves impossible due to a lack of current contact information for the data subject concerned.

(3) The Provider shall not voluntarily disclose personal data to law enforcement or government authorities without a valid legal procedure, except in urgent situations.

Art. 21 - Prohibition on the sale of personal data

(1) The Provider expressly declares that personal data processed through the Platform shall never be sold, rented, licensed for monetary compensation, or otherwise transferred to third parties for their own commercial purposes. This prohibition applies regardless of whether the data is anonymized, aggregated, or pseudonymized.

(2) For the purposes of paragraph (1), "sale" covers any disclosure of personal data to third parties in exchange for monetary or other compensation, including, but not limited to:

1. Direct financial payments;
2. Exchange of personal data for services, marketing opportunities, or business advantages;
3. Revenue-sharing arrangements where data sharing directly or indirectly contributes to revenue generation;
4. Bartering arrangements involving data transfers;
5. Any other transfer creating economic benefit for the Provider beyond reasonable compensation for providing contracted services.

(3) The prohibition in paragraph (1) does not prevent the following permitted transfers, which do not constitute "sales" under applicable data protection laws:

1. Disclosures to service providers and sub-processors under Article 18, provided such entities process data solely on behalf of the Provider according to documented instructions;
2. Business transfers under Article 19 involving mergers, acquisitions, or corporate reorganizations;
3. Legal disclosures under Article 20 responding to valid legal process or mandatory legal obligations;
4. Disclosures made with explicit consent under Article 17(5), where data subjects have been clearly informed that their data will be shared for third-party purposes and have provided affirmative opt-in authorization;
5. Aggregate, anonymized statistical information that cannot reasonably be used to identify specific individuals.

(4) California residents and residents of other US states with applicable privacy laws possess statutory rights to opt out of data sales even though the Provider does not engage in such sales. The Provider also recognizes and honors browser-based opt-out preference signals, including Global Privacy Control (GPC), and treats such signals as valid Do Not Sell or Share requests under applicable US state privacy laws.

(5) The Provider commits to maintaining the no-sale policy established in this Article indefinitely. Any future change to this policy would require:

1. Amendment to this Privacy Policy with prominent notice under Article 38;
2. Obtaining explicit opt-in consent from all affected data subjects;
3. Provision of clear opt-out mechanisms allowing data subjects to exclude themselves from any sales programs;
4. Compliance with all applicable statutory requirements governing data sales, including California Consumer Privacy Act, Virginia Consumer Data Protection Act, and equivalent state laws.

SECTION VII - INTERNATIONAL TRANSFERS & LOCALIZATION

Art. 22 - Cross-Border Transfers and Safeguards

(1) Personal data collected through the Platform is transferred to and processed in the United States of America, where the Provider maintains primary infrastructure and operations. Business customers located outside the United States and data subjects whose information is processed through the Platform acknowledge and consent to such international transfers as necessary for service delivery.

(2) The Provider utilizes Amazon Web Services infrastructure with primary hosting in US-East-1 (Northern Virginia) and US-West-2 (Oregon) regions. Additional regional hosting options are available per Article 23 for customers requiring data localization to specific jurisdictions.

(3) International data transfers from the European Economic Area to the United States are governed by Standard Contractual Clauses approved by the European Commission pursuant to GDPR Article 46(2)(c). The Provider has executed these Standard Contractual Clauses with all sub-processors receiving personal data originating from EEA (European Economic Area) data subjects. Copies of executed Standard Contractual Clauses are available upon request through the contact channels specified in Article 39.

(4) For transfers from the European Economic Area, the Provider has conducted Transfer Impact Assessments evaluating risks associated with processing personal data in the United States. These assessments consider:

1. US surveillance laws and their potential application to data processed through the Platform;
2. Legal remedies available to data subjects under US law;
3. Supplementary technical and organizational measures implemented to mitigate identified risks;
4. Specific characteristics of the data being transferred and sensitivity levels;
5. Purposes and contexts of processing activities.

(5) Supplementary measures implemented to strengthen Standard Contractual Clauses include:

1. End-to-end encryption of data in transit using the TLS 1.3 protocol;
2. At-rest encryption using AES-256 encryption for all stored personal data;
3. Minimization of data transmitted to what is strictly necessary for the provision of the service;
4. Contractual prohibitions that prevent subcontractors from disclosing data to government authorities without notification from the Provider, except where this is legally impossible;
5. Regular security audits and penetration tests of the infrastructure;
6. Immediate notification of affected business customers upon receipt of data access requests from government authorities, subject to legal restrictions on such notifications.

(6) International transfers to AI providers are governed by the following framework:

1. OpenAI, Inc. operates under the standard contractual clauses for data transfers in the EEA and maintains infrastructure in multiple regions;
2. Anthropic PBC operates under the standard contractual clauses for data transfers in the EEA;
3. Data transmitted to AI providers is limited to the text content necessary to generate the requested results, systematically excluding metadata and identifiers where technically possible;

(7) The provider monitors legal and regulatory changes affecting international data transfers, including adequacy decisions, updates to standard contractual clauses, and court rulings affecting transfer mechanisms. Significant changes to transfer safeguards result in notification to affected business customers within 30 days.

(8) Data subjects whose personal data is transferred internationally retain all rights set out in Sections X to XII, regardless of the location of processing. Geographical transfer does not diminish the rights of access, rectification, erasure, restriction, portability, objection, or complaint to supervisory authorities.

Art. 23 - Data Localization in India and Regional Hosting

(1) The Provider offers hosting in the India region through the Amazon Web Services Mumbai (ap-south-1) for business customers who are subject to data localization requirements under the Digital Personal Data Protection Act of 2023 or contractual obligations requiring data storage in the country.

(2) Hosting in the India region operates under the following parameters:

1. All customer account data, applicant information, employee records, and artificial intelligence processing results are stored exclusively within India;
2. Database replication and backup systems store copies only in the AWS Mumbai infrastructure;
3. Platform servers processing data hosted in India operate from Indian data centers;
4. Cross-border transfers are only performed when technically necessary for specific operations and only with the express permission of the customer.

(3) Exceptions to full data localization under paragraph (2) include:

1. Artificial intelligence processing requests submitted to OpenAI or Anthropic infrastructure, which may process data outside India. Business customers must explicitly consent to such transfers through account configuration, confirming that the functionality of artificial intelligence requires international data transfers;
2. Payment processing operations handled by international payment processors necessary for billing subscriptions and financial transactions;
3. Email delivery services that route messages through international infrastructure to reach recipients located outside India;
4. Sharing security threat information with global security service providers to detect malware, prevent attacks, and manage vulnerabilities;
5. Legal disclosures to authorities outside India when required by valid legal process meeting the standards set forth in Section 20.

(4) The Provider shall monitor regulatory guidance issued by the Data Protection Board of India and update data localization practices as required by law. If new mandates impose stricter localization requirements, the Provider shall:

1. Notify affected business customers within 90 days of regulatory clarification;
2. Implement technical modifications necessary for compliance within commercially reasonable timeframes;
3. Offer customers options to migrate to compliant configurations or terminate subscriptions without penalty if compliance proves technically or economically infeasible;

4. Maintain transparent communication regarding implementation timelines and any service limitations resulting from compliance measures.

(5) The Provider does not process personal data through infrastructure located in jurisdictions subject to comprehensive sanctions imposed by the United States, European Union, or United Nations Security Council. Business customers located in or processing data from sanctioned territories must seek explicit written authorization before Platform access, which may be denied based on legal compliance requirements.

SECTION VIII - DATA RETENTION AND DELETION

Art. 24 - Storage periods and deletion schedules

(1) The Provider shall store personal data for the minimum period necessary to fulfill the purposes for which it was collected and to protect business interests or legal requirements. Retention periods vary depending on the category of data, the purpose of processing, and applicable legal requirements.

(2) Customer account data shall be retained as follows:

1. *Active subscription period:* All account information, including registration details, payment methods, subscription configurations, and usage history, is retained for the entire active subscription period.
2. *Post-termination retention period:* Account data remains accessible for 30 days after subscription termination to allow for data export and account reactivation if customers reverse their termination decision;
3. *Financial records retention:* Billing information, payment transaction records, invoices, and related financial documentation are retained for 7 years after the fiscal year in which the transactions occurred, in accordance with the requirements of the tax authorities in the US and India;
4. *Disputed accounts:* When investigating or litigating disputes regarding billing, refunds, legal claims, or violations of the Terms and Conditions, account data is retained until the dispute is finally resolved, plus the applicable statute of limitations.

(3) Candidate and employee data uploaded by business customers is retained according to the following schedule:

1. *During active subscription:* Business customers exercise full control over the storage and deletion of candidate data through the platform's features, with the provider storing this data for an indefinite period while subscriptions remain active, unless customers delete the records at their discretion;
2. *After subscription termination:* Upon termination of the subscription, candidate and employee data enters the 30-day retrieval window specified in paragraph (2), during which business customers can export or retrieve all stored information;

(4) Technical and usage data is stored according to the following parameters:

1. *Server logs and access records:* These are stored for 90 days from the date of creation to assist with security monitoring, troubleshooting, and performance optimization.
2. *Security incident data:* Logs and information related to security events, breach investigations, or threat detection activities are stored for 2 years to enable pattern analysis and demonstrate compliance;
3. *Aggregated analytics data:* Anonymized usage statistics that are not linked to specific individuals are retained for a period of 3 years for the purpose of developing new products and services;
4. *Error reports and diagnostic data:* These are stored for 180 days or until the underlying issues are resolved, whichever occurs first.

(5) Data processed by artificial intelligence is subject to the following storage rules:

1. *Commands entered and content uploaded:* Transmitted to artificial intelligence providers solely for the purpose of generating results and not stored by the Provider after the expiration of the customer account storage period, with artificial intelligence providers contractually obligated to delete entered commands within 30 days;
2. *Results generated by AI:* These are stored in accordance with the business customer account storage schedules in paragraphs (2) and (3), as these results are the property of the customer;
3. *AI processing logs:* Metadata recording which AI features were used, processing timestamps, and errors encountered are stored for 90 days for troubleshooting and service quality monitoring.

(6) Marketing and communication data follows the following retention periods:

1. *Marketing consent records:* stored for 2 years from the time of consent
2. *Email communication records:* email transaction records are stored for 2 years; marketing email records are stored for 1 year
3. *Support ticket correspondence:* retained for 2 years after ticket closure to assist with quality assurance, training, and dispute resolution.

(7) Legal hold procedures take precedence over standard retention schedules when:

1. Valid legal process requires data preservation for litigation, investigation, or regulatory proceedings;
2. The Provider reasonably anticipates legal claims, regulatory inquiries, or audit proceedings where data would be relevant;
3. Business customers notify the Provider of their own legal hold obligations affecting data stored on the Platform.

Art. 25 - Post-Termination Data Handling

(1) Upon subscription termination initiated by either the Provider or business customers, the following sequence governs data handling:

1. *Termination effective date:* The subscription terminates and Platform access is immediately restricted to read-only mode, preventing creation of new records or modification of existing data;
2. *Retrieval window commencement:* A 30-day period begins during which customers retain login access specifically for data export and retrieval purposes;
3. Export functionality: Self-service export tools remain available throughout the retrieval window, enabling download of all customer data in machine-readable formats including CSV or JSON depending on data type;
4. *Deletion warning notifications:* Automated reminders are sent to account administrators at 30 days, 15 days, and 3 days before permanent deletion;
5. *Permanent deletion:* At retrieval window expiration, all customer data is deleted from active systems and marked for removal from backups.

(2) Bulk data transfer arrangements are available for business customers with large data volumes exceeding practical limits for self-service export. Customers must submit bulk transfer requests within the first 15 days of the retrieval window to allow adequate processing time. Bulk transfers occur via:

1. Secure File Transfer Protocol connections to customer-designated servers;
2. Encrypted external storage media physically shipped to customer addresses;
3. Direct API connections enabling automated data extraction by customer systems if its possible;

(3) The Provider implements secure deletion procedures meeting industry standards for data destruction:

1. Active database records are overwritten with random data patterns before deallocation;
2. File storage systems employ cryptographic erasure by destroying encryption keys, rendering data mathematically unrecoverable;
3. Backup media undergoes secure overwriting or physical destruction at end of lifecycle;
4. Deleted data does not migrate to archival storage or offline backup systems;
5. Deletion completion certificates are issued to enterprise customers upon request, documenting destruction of specified data categories.

(4) Retrieval window extension requests must be submitted before the original retrieval period expires. Requests received after permanent deletion has occurred cannot be accommodated, as deleted data is technically irrecoverable.

(5) Customers who terminate subscriptions and later wish to resume Platform use must create new accounts following standard registration procedures. Previous accounts and data are not restored. Reactivation is treated as new customer acquisition unless:

1. Termination was initiated by the Provider in error;
2. Reactivation occurs within the 30-day retrieval window before permanent deletion;

3. Enterprise customers with contractual provisions establishing different reactivation terms.

(6) The Provider reserves the right to deny new account registration to individuals or organizations whose previous accounts were terminated for Terms & Conditions violations, fraud, abusive conduct, or other material breaches. This denial right extends indefinitely and is not subject to appeal, though affected parties may submit written explanations for reconsideration at legal@peoplebotapp.com

SECTION IX - SECURITY MEASURES

Art. 26 - Technical Security Controls

(1) The Provider implements comprehensive technical security measures designed to protect personal data against unauthorized access, disclosure, alteration, and destruction. These measures are regularly reviewed, tested, and updated to address evolving threat landscapes and maintain alignment with industry best practices.

(2) Sensitive data is safeguarded using the latest encryption methods, ensuring both the security of transmitted information and that stored in databases. To further protect this data, access is granted only to personnel who require it for operational purposes, and this is tightly controlled. Additionally, the security infrastructure benefits from continuous monitoring, including firewalls and real-time intrusion detection, aimed at proactively addressing any vulnerabilities.

(3) In the same vein, all employees undergo comprehensive security training upon hiring, as well as refresher courses on an annual basis. Those entrusted with handling personal data are bound by stringent confidentiality agreements. Third-party vendors are scrutinized rigorously and must meet the Provider's exacting security standards before engaging in any processing activities.

Art. 27 - Organizational Security Measures

(1) The Provider has established a set of comprehensive organizational policies and procedures designed to ensure that technical and administrative security controls are consistently applied and continuously improved in relation to the processing of personal data. These measures are reviewed on a regular basis to adapt to new risks, regulatory changes, and evolving technologies.

(3) The Provider's personnel security practices include the following:

1. **Background Checks**: All employees who have access to personal data undergo thorough background checks, including verification of previous employment, education credentials, and criminal record checks, where applicable.
2. **Confidentiality Agreements**: Every employee is required to sign a confidentiality agreement before receiving access to systems or personal

data, with obligations extending beyond the termination of employment.

(4) The Provider ensures compliance with security practices through regular audits and reviews of security measures, including:

1. **Internal Audits**: Annual internal audits are conducted to assess the effectiveness of security controls, identify areas for improvement, and ensure compliance with internal policies and legal requirements.
2. **External Audits**: Independent third-party audits and penetration tests are carried out annually to assess vulnerabilities, identify risks, and ensure that security standards are met.

(5) Security measures related to third-party vendors and subprocessors include the following:

1. **Vendor Management**: All third-party vendors with access to personal data must undergo security assessments before engagement. This includes evaluating the vendor's security policies, reviewing contracts, and, where necessary, conducting on-site audits;
2. **Vendor Access Restrictions**: Data access is restricted to the minimum required to perform contracted services, and access is regularly reviewed to ensure compliance with security agreements.
3. **Termination of Vendor Access**: In the event of contract termination or suspension, all personal data must be returned or destroyed, and access to the systems is revoked within 48 hours.

Art. 28 - Data Breach Response and Notification

(1) When an incident is detected, the Provider's response is immediate and methodical. Each breach is meticulously investigated to understand the extent of the compromise, the specific data involved, and the potential consequences for the data subjects. Swift, decisive action is taken to prevent further damage, all while ensuring full adherence to legal obligations.

(2) In cases where a data breach is confirmed, the Customer will be notified without unnecessary delay. The notification will include all relevant details, enabling the Customer to fulfill their obligations, including the GDPR's 72-hour reporting requirement. Should other laws apply- such as the Indian Digital Personal Data Protection Act or applicable state laws in the US- the Provider will adhere to those notification deadlines as well.

(3) The Customer will receive a clear and comprehensive breakdown of the breach, including information about the nature of the incident, the types of data affected, and the estimated number of individuals impacted. To mitigate any negative effects, the Provider will also explain the actions taken to rectify the situation and prevent any recurrence.

(4) As the Data Controller, it is the Customer's responsibility to communicate with affected employees or candidates, in accordance with relevant legal requirements. To assist with this, the Provider will provide all necessary documentation and support to facilitate the dissemination of breach-related information.

(5) Throughout the investigation process, the Provider will work in close collaboration with the Customer and the relevant authorities. Full support will be given to ensure the Customer can comply with their own reporting obligations. If required by law enforcement, public notifications may be delayed to protect the integrity of ongoing investigations.

SECTION X - PRIVACY RIGHTS

Art. 29. Core Data Subject Rights (GDPR Focus)

(1) Individuals whose Personal Data is processed by the Platform (referred to as the "Data Subject") possess a comprehensive set of legally enforceable privacy rights derived from the General Data Protection Regulation (GDPR).The Provider facilitates the immediate and effective exercise of these rights through the specialized request procedures detailed in Article 33 (Data Subject Request Procedure).

(2) The Data Subject may request confirmation whether the Provider processes the Data Subject's Personal Data. If processing is confirmed, the Data Subject is entitled to receive a complete copy of the data. The response shall specify the exact processing purposes, the categories of data processed, the retention period, and information regarding the right to lodge a complaint. The first copy is provided free of charge. Subsequent, manifestly unfounded or excessive requests may be subject to a reasonable administrative fee reflecting the costs of provision.

(3) The Data Subject may request the prompt correction of inaccurate Personal Data and the completion of incomplete data relevant to the processing purpose.The Provider shall implement verified corrections within the legally mandated timeframe of 30 days and notify all third-party recipients of the correction, unless this proves impossible or involves a disproportionate effort.

(4) The Data Subject may request the erasure of Personal Data under specific conditions, primarily when:

1. The data is no longer necessary for the original purpose;
2. Consent has been withdrawn (where consent was the sole legal basis); or
3. The Data Subject successfully objects to processing based on legitimate interests.

Exceptions: This right is not absolute. Retention is mandatory when processing is necessary for compliance with a mandatory legal obligation, reasons of substantial public interest or the establishment, exercise, or defense of legal claims. Erasure protocols shall cover both active systems and secure backup media, consistent with the Controller's approved retention schedule.

(5) The Data Subject may request the restriction (i.e., storage only, without active processing) of data when:

1. The accuracy of the data is contested; or
2. The processing is unlawful, and the Data Subject opposes erasure; or
3. The Provider no longer requires the data, but the Data Subject requires it for the defense of legal claims. (b) The restriction shall be lifted once the underlying dispute is resolved, and the Data Subject shall be notified before the resumption of any processing.

(6) This right applies only to data actively provided by the Data Subject, where processing is based on consent or a contract, and is performed by automated means. The data shall be provided in a structured, commonly used, and interoperable machine-readable format (e.g., CSV or JSON), facilitating easy transfer. Where technically feasible, the Data Subject has the right to request the direct transmission of the Data Subject's data from the Provider to another designated controller without hindrance.

(7) The Data Subject has the unconditional right to object to processing for the purposes of direct marketing, including related profiling. This objection shall be honored immediately and permanently. The Data Subject may object to processing based on the Controller's stated legitimate interests. The Controller shall promptly cease processing unless it can demonstrate compelling legitimate grounds that clearly override the specific interests, rights, and freedoms of the Data Subject.

(8) The Data Subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significant impacts for the Data Subject. The Platform does not utilize fully automated decision-making processes that produce such significant legal effects. Any AI-generated suggestions are subject to human review and contextual analysis and do not constitute a final, substantial decision. The Data Subject retains the right to request human intervention and challenge any such output.

Art. 30. India-Specific Rights (Digital Personal Data Protection Act 2023)

(1) These provisions apply specifically to Data Subjects located in India (referred to as the "Data Principal"), or whose Personal Data is processed in relation to the Controller’s operations within India.

(2) The Data Principal is entitled to obtain a summary of the processing activities, the categories of Personal Data processed, and information regarding the involved Data Fiduciaries and Processors, presented in clear and accessible language.

(3) Requests for correction of inaccurate or misleading data must be implemented within 15 business days. Erasure shall occur when the data is no longer necessary for the purpose for which it was collected, or upon withdrawal of consent.

(4) All concerns regarding processing activities shall be addressed to the designated Grievance Officer. An acknowledgement of the grievance shall be issued within 48 hours, and a substantive, detailed response shall be provided within 30 days. The Data Principal has the right to nominate another individual to exercise the Data Principal's rights in the event of death or incapacity.

(5) Verifiable parental or guardian consent is a mandatory requirement before processing the Personal Data of a child (under 18 years old). Data discovered to belong to a minor without such consent shall be suspended and promptly deleted within the shortest operational cycle possible.

Art. 31. US State Privacy Rights (CCPA/CPRA, VCDPA, CPA, etc.)

(1) Residents of states such as California, Virginia, Colorado, Connecticut, and Utah are granted specific rights regarding their Personal Information, collectively referred to as Consumer Rights. These rights operate independently of the GDPR rights.

(2) The Controller does not engage in the traditional "sale" of Personal Information for monetary compensation. Consumers maintain the right to Opt-Out of Sharing Personal Information for the purpose of cross-context behavioral advertising (targeted advertising). This is managed via the designated "Do Not Sell or Share My Personal Information" link on the Platform's footer

(3) Consumers have the right to limit the use and disclosure of Sensitive Personal Information. The Controller utilizes SPI only for purposes strictly necessary to perform the services requested by the Consumer.

(4) The Controller guarantees that Consumers shall not face any discrimination (including price or service quality differentials) for exercising any of the Consumer's privacy rights. If a request is denied, the Consumer has the right to appeal the decision. The appeal must be submitted within 30 days of receiving the denial, and the Controller shall provide a final, substantive response to the appeal within 60 days.

(5) Consumers may utilize an Authorized Agent to submit a verifiable request on the Consumer's behalf, provided that the Agent presents satisfactory written proof of the Consumer’s signed permission to act on the Consumer's behalf.

Art. 32 - Specific rights of candidates and employees

(1) Candidates and employees whose personal data is processed through the Platform by business customers acting as data controllers have all the rights described in Articles 29 to 31, depending on the jurisdiction of their place of residence. These rights are exercised primarily through the business customer who controls their data, although the Provider assists in the fulfillment of requests when technically necessary and in accordance with the Provider's role as a personal data processor.

(2) Applicants have the right to be informed that artificial intelligence assists in the processing of their application documents and that recommendations generated by artificial intelligence influence but do not determine hiring decisions. Business customers are responsible for providing this notice at the time of data collection or before the start of processing by artificial intelligence. The notice should describe the function of the artificial intelligence, confirm that human decision-makers review the results of the artificial intelligence before making hiring decisions, and explain how candidates can object to automated processing where required by law. The provider shall provide notification templates and technical mechanisms to assist customers in complying with their notification obligations.

(3) The right to human review allows candidates to request that hiring decisions affecting them include meaningful human assessment rather than being based primarily on automated results.

(4) The rights to object to automated processing are exercised by contacting the business customer who uploaded the candidate's information or, if the business customer does not respond or is unknown, by contacting the provider through the channels specified in Article 33. The provider shall forward the objections to the relevant business customers and provide technical assistance to remove the objecting candidates from the automated processing workflows.

(5) The rights to rectification shall apply when candidates identify inaccuracies in the personal data uploaded to the platform by business customers. Corrections shall be submitted to business customers with supporting documentation justifying the claimed corrections, such as updated CVs, corrected transcripts, or explanatory notes clarifying misunderstandings. Business customers evaluate requests for correction and instruct the Provider to apply the verified corrections. Where business customers dispute correction requests or delay them unreasonably, applicants may turn to the Provider, who investigates and, where appropriate, applies the corrections in accordance with its independent data protection obligations.

(6) The Provider supports the exercise of employee rights by providing employers with tools to extract employee data, document processing activities, and demonstrate compliance with human oversight requirements.

Art. 33 - How to exercise your rights

(1) The rights set out in Articles 29 to 32 shall be exercised by submitting written requests to the Provider or, for candidates and employees, to the business customer who controls their data. Requests shall specify which right is being exercised, provide sufficient information to identify the data subject, and include any supporting documentation necessary to verify and process the request.

(2) Requests submitted to the Provider shall be addressed to legal@peoplebotapp.com or sent by mail to PeopleBotApp, Inc. Requests must include the data subject's full name, email address associated with the Platform accounts, if applicable, sufficient additional information to locate the relevant data, and a clear description of the right being exercised and the actions requested. Incomplete requests will receive a response requesting additional information necessary for processing, and the deadline for response will be postponed until sufficient information is provided.

(3) Identity verification is performed prior to the execution of rights requests to prevent unauthorized access to personal data or the unlawful exercise of rights affecting legitimate data subjects. Verification standards balance security and accessibility by requiring information that is reasonably accessible to legitimate data subjects but difficult for imposters to obtain. Standard verification requests include email addresses associated with accounts, answers to pre-set security questions, or presentation of government-issued identification documents with sensitive data redacted. Enhanced verification may be required for sensitive requests, such as downloading complete account data or deleting accounts with significant transaction history.

(4) Requests submitted by authorized representatives require proof of authority through signed powers of attorney, proxy documents, or registration with government agencies where applicable law establishes representative registration systems. Representatives must provide their identification along with proof of their authority to act on behalf of the data subject.

(5) Response times vary depending on the jurisdiction and type of request, but generally comply with the following standards. Access and portability requests are responded to within 30 days, with the possibility of an extension to 60 days for complex or voluminous requests, in which case a notice of extension is provided. Rectification requests are processed within 30 days of confirmation. Requests for deletion and restriction are fulfilled within 30 days, provided that the grounds for deletion or restriction are confirmed. Objections are processed immediately for marketing-related objections and within 30 days for objections based on legitimate interests. Withdrawal of consent takes effect within 72 hours or immediately, where technically possible.

(6) Responses to requests for rights shall indicate the actions taken, provide the requested data where applicable, explain any refusals with reference to specific legal exceptions, inform data subjects of their rights to lodge complaints with supervisory authorities, and provide contact information for follow-up questions. Partial fulfillment shall be provided when some of the requested actions can be fulfilled and others cannot, with a clear explanation distinguishing the fulfilled and rejected components of the request. Refusals are never general, but refer to specific reasons why specific legal exceptions apply to the situation of the data subject making the request.

(7) Candidates and employees whose data is controlled by business customers should submit rights requests directly to those customers in the first instance. Business customers are typically in a better position to respond comprehensively, given their role as data controllers and their direct relationship with candidates and employees. Where business customers fail to respond within 45 days or refuse requests in an inappropriate manner, the individuals concerned may contact the Provider, who will investigate and, where the Provider has obligations as a data processor to facilitate the exercise of rights, implement appropriate measures to ensure compliance with the rights.

(8) The rights of complaint exist independently of the request procedures described above. Data subjects who are not satisfied with the Provider's response to requests for rights or who are concerned about data protection practices may lodge complaints with the supervisory authorities referred to in Article 40, seek judicial redress in the competent courts, or seek alternative dispute resolution through mechanisms offered by the Provider or required by applicable law.

SECTION XI - SPECIAL TOPICS

Art. 34 - Children's Privacy and Age Restrictions

(1) The Platform is not intended for use by persons under the age of eighteen. Account registration requires confirmation that users are of legal age in their jurisdiction. The provider does not knowingly collect or process personal data of minors.

(2) Accounts suspected of belonging to minors are subject to verification, which requires a government-issued ID card or equivalent document. Confirmed accounts of minors will be terminated within 48 hours and all related data will be deleted within 30 days.

(3) Business customers are responsible for ensuring that the data uploaded for candidates or employees relates only to persons who meet the minimum age for employment in the applicable jurisdictions. The provider is not responsible for compliance with labor laws regarding underage workers.

Art. 35 - Automated decision-making and transparency of artificial intelligence

(1) The platform functions as a recommendation mechanism to assist human decision-making, not as a means of autonomous decision-making for employment. This design reflects the legal requirements under Article 22 of the GDPR, the provisions of the Indian DPDP Act, and ethical commitments to preserve human judgment in hiring processes.

(2) Artificial intelligence generates candidate compatibility scores, rankings, skill summaries, content suggestions, and analytical insights. All results are labeled as recommendations, not final decisions. User interfaces constantly remind business customers that final decisions remain their responsibility.

(3) Fully automated hiring decisions are prohibited through contractual restrictions, technical safeguards that prevent mass automated actions, and a requirement for human confirmation before finalizing important decisions. Audit logs record which users reviewed the recommendations, the duration of the review, the changes made, and the final decisions.

(4) Business customers must implement documented oversight procedures that establish reviewer qualifications, sources of information beyond AI results, required review time, documentation standards, and quality monitoring. The provider offers guidance, but customers are responsible for adequate procedures.

(5) The provider maintains transparency regarding the capabilities and limitations of AI through its AI Transparency and Use Policy, which details the AI models used, training data sources, known limitations, bias testing procedures, and model update practices. This policy is available at https://www.peoplebotapp.com/ai-usage and is updated when significant changes occur.

(6) Ownership rights over the results of artificial intelligence do not override the legal restrictions on automated decision-making set out in this Article. Business customers own content generated by artificial intelligence in accordance with Article 16, but must comply with human oversight requirements when using such content for recruitment purposes.

Art. 36 - Third-party services and external links

(1) The platform supports integrations with third-party services, including applicant tracking systems, human resources information systems, communication platforms, calendar applications, and productivity tools. Each integration requires explicit permission from the customer, specifying the permissions for data access.

(2) Data shared with integrated services becomes subject to the privacy policies, terms of use, and data processing practices of those services. The provider conducts security assessments before activating integration partnerships, but cannot control third-party practices with respect to data after it has been transferred.

(3) Integration permission can be revoked at any time through account settings. Revocation prevents future data sharing but does not delete data that has been transferred to the integrated services. Customers must contact the integrated service providers directly to request deletion of previously shared data.

(4) The Platform may contain links to external websites, resources, or services that are not operated by the Provider. These links are provided for convenience only and do not constitute an endorsement of the linked content or affiliation with the linked entities. External sites operate under their own privacy policies.

(5) The Provider is not responsible for the privacy practices, content accuracy, security measures, or data processing of third-party services or linked websites. Customers access external services at their own risk and should review the applicable privacy policies before providing personal data.

Art. 37 - Marketing Communications and Opt-Out

(1) The Provider shall only send marketing communications to persons who have given their consent to be included, or to existing customers regarding similar services, where permitted by applicable law. Marketing communications include promotional content about new features, service improvements, educational resources, and special offers.

(2) Consent for marketing communications shall be obtained through clear opt-in mechanisms during account registration. Consent requests shall identify specific types of communications, frequency expectations, and opt-out procedures. Pre-checked boxes do not constitute valid consent for marketing communications.

(3) Each marketing communication contains clear unsubscribe mechanisms that allow for immediate opt-out. Unsubscribe links appear at the bottom of emails and are processed with a single click, without requiring account login or additional information beyond confirmation of the intent to unsubscribe. Unsubscribe requests are processed within 48 hours.

(4) Transactional messages are not affected by the unsubscription from marketing messages. Account-related communications, including password resets, billing confirmations, security alerts, subscription status notifications, and service updates, continue regardless of marketing preferences, as these communications are necessary for the provision of services and not for promotional purposes.

(5) The frequency of marketing communications is managed to avoid excessive communication that could be considered spam or harassment. The standard frequency ranges from weekly to monthly, depending on subscription preferences.

(6) The Provider does not share email addresses or contact information with third parties for their independent marketing purposes. Service providers that assist in the delivery of emails operate under strict confidentiality and usage restrictions that prevent unauthorized use for marketing purposes.

(7) Marketing message opt-out preferences are honored across all of the Provider's communication channels, including email, SMS where applicable, notifications, and in-app messages. No separate opt-outs are required for each channel, with universal preferences applied unless customers specify preferences for a specific channel.

SECTION XII - POLICY UPDATES AND CONTACTS

Art. 38 - Changes to this Privacy Policy

(1) The Provider reserves the right to change this Privacy Policy at any time to reflect changes in legal requirements, business practices, service features, data processing activities, or security measures.

(2) Significant changes affecting the rights of data subjects, the purposes of processing, the categories of data collected, the categories of recipients, the storage periods, or international transfer agreements will result in prior notification to the affected parties. The notification shall be provided at least 15 days before the changes take effect by email to the registered account addresses, by banners prominently displayed on the Platform interface or on social networks, and by publishing updated versions of the policy on the Provider's website. Minor changes, such as clarifications, formatting improvements, or updates to contact information, may be implemented without prior notice.

(3) Notification emails shall specify the specific sections that have been changed, summarize the key changes in accessible language, provide links to the current and updated versions of the policy with changes highlighted, and explain the reasons for the changes. Business customers will receive additional notification when the changes affect their obligations under the Data Processing Addendum or alter the Provider's agreements with its subcontractors.

(4) Use of the platform after the effective date of the policy changes is deemed acceptance of the changes. Customers who find the changes unacceptable may terminate their subscription before the effective date without penalty and receive a pro-rated refund for the unused portion of their prepaid subscription. For changes that require new consent under applicable law, such as expanding the purposes of processing or adding new data recipients, the provider shall obtain explicit consent to participate before implementing the changes.

(5) The provider maintains a history of versions of this Privacy Policy through numbered versions, effective dates clearly indicated in the document header, change logs summarizing changes between versions, and archived copies of previous versions. Version control allows data subjects, business customers, and regulatory authorities to track the evolution of the policy and verify the commitments applicable during specific periods of time.

(6) Urgent changes may be made without 15 days' notice where required by court orders, regulatory directives, security incidents requiring immediate protective measures, or events of force majeure. Urgent changes shall be communicated immediately after their implementation, with explanations given for the urgency justifying the shortened notice periods.

Art. 39 - Contact Information and Privacy Inquiries

(1) General privacy inquiries, questions about this Privacy Policy, requests for additional information about data processing practices, and concerns about potential privacy violations should be sent to legal@peoplebotapp.com. Email inquiries will receive confirmation within 3 business days and substantive responses within 15 business days. Complex inquiries requiring investigation may take up to 30 days, with interim status updates provided.

(2) Data subject rights requests shall be submitted to legal@peoplebotapp.com. The processing of rights requests shall be carried out in accordance with the procedures and timeframes set out in Article 33. Requests should contain sufficient information to identify the data subject and verify the legitimacy of the request prior to processing.

(3) Security incident reports and vulnerability disclosures shall be submitted to legal@peoplebotapp.com and shall receive immediate attention from security personnel. The provider maintains coordinated vulnerability disclosure procedures that allow security researchers to report potential vulnerabilities confidentially without incurring legal liability.

(4) Support for business customers on privacy-related issues, including questions about this data processing policy, subcontractor objections, assistance with candidate rights requests, and technical issues affecting data protection compliance, is available at legal@peoplebotapp.com. Corporate customers with dedicated account managers may also contact their designated representatives directly.

Art. 40 - Complaints Officers and Regional Representatives

(1) The Complaints Officer shall respond to complaints within 48 hours and resolve complaints within 30 days or provide an update on the status explaining any delays in resolution.

(2) Complaints that are appropriate for the India Complaints Officer include complaints regarding the processing of core Indian data information, requests for assistance in exercising rights under the DPDP Act, concerns about consent mechanisms or data localization practices, and disputes regarding business customers' responses to candidate or employee rights requests. The complaints officer coordinates with business customers acting as data controllers to facilitate the resolution of issues that are under the control of the customers.

(3) The provider monitors regulatory guidance on representative appointment requirements and appoints representatives where required by law. At the time of these general terms and conditions taking effect, there is no obligation to appoint a data protection officer.

(4) Data subjects retain their right to lodge complaints directly with supervisory authorities, regardless of the internal complaint procedures described in this article. The relevant supervisory authorities include the Data Protection Council of India for matters concerning Indian data subjects and the Federal Trade Commission in the United States with powers to enforce data protection laws. The contact information for the supervisory authorities is published on their respective websites and in official government directories.

(5) The provider shall cooperate fully with investigations by supervisory authorities, respond to requests for information within the specified time limits, provide the requested documentation and access to data, implement corrective measures imposed through enforcement actions, and maintain transparent communication during the investigation and resolution process.

(6) Updates to the contact information in this Article and Article 39 do not constitute material policy changes requiring 15 days' notice under Article 38. Updates to the contact information shall take effect immediately upon publication of a notice through the standard communication channels. Outdated contact information shall continue to be monitored for a reasonable transition period to prevent loss of communication during the transition of contacts.