



**PRIVACY NOTICE TO CALIFORNIA JOB APPLICANTS, EMPLOYEES, EMERGENCY CONTACTS, AND BENEFICIARIES
REGARDING THE COLLECTION OF PERSONAL INFORMATION**

Pinnacle Group and its affiliates (“Pinnacle” or “Company”) are committed to protecting the privacy and security of personal information of its job applicants, employees and their emergency contacts and beneficiaries. Pinnacle with the California Privacy Rights Act (CPRA) and all data privacy and laws in the jurisdictions in which it recruits and hires employees.

This Notice describes how Pinnacle collects, discloses, and uses your personal information as part of our business operations, including when you apply for a job, accept an offer of employment, are an emergency contact or beneficiary, or are engaged as an independent contractor of Pinnacle or one of our clients. We collect only the personal information that is reasonably necessary and proportionate to achieve our purposes. We do not sell your personal information. We also do not share/disclose any personal information for purposes other than are those permitted under the CPRA and as described in this notice.

Personal Information We Collect

Below are the types of personal information we may collect from you and/or about you, and examples of each:

- **Identifying information** (such as full name, alias, gender, date of birth, and signature).
- **Demographic data and protected categories** (such as race, ethnic origin, gender, marital status, disability, veteran or military status, and status as a victim of domestic violence, assault, or stalking).
- **Contact information** (such as postal address, telephone numbers, email address, and emergency contact information).
- **Dependents’ information** (such as name, address, date of birth, and Social Security numbers (SSN)).
- **National identifiers** (such as SSN, driver’s license number, state identification number, passport and visa information, and other similar identifies are well as immigration status and documentation).
- **Educational and professional background** (such as work history, academic and professional qualifications, educational records, and references).
- **Employment details** (such as job title, position, hire dates, compensation, performance and disciplinary records, and vacation and sick leave records).
- **Financial information** (such as banking details, tax information, payroll information, and withholdings).
- **Health and Safety information** (such as health conditions relevant to your employment, workplace illness and injury information, and health insurance policy information).
- **Information relating to use of Company IT systems** (such as search and browsing history, login information, and IP addresses on the Company's information systems and networks).
- **Geolocation data** (such as time and physical location related to use of an internet website, application, device, or physical access to a Company office location).
- **Testing data** (such as summary about preferences, characteristics, attitudes, intelligence, abilities, and aptitudes).
- **Other information** (such as voluntary information you may provide to Pinnacle in the course of your interactions with us).

Why We Collect Personal Information And With Whom Is It Shared

Our business purposes for collecting and using your personal information include human resources, employment, benefits administration, health and safety, compliance, and to establish and exercise our legal and contractual rights. Many of these business purposes require that we disclose your personal information internally (e.g. human resource and IT personnel) and to third parties such as clients and service providers (e.g. benefits administrators and insurance companies). We may also share or disclose personal information as required or permitted by law, including sharing with governmental agencies, law enforcement, or other third parties in litigation or legal disputes. We do not, however, “sell” your personal information within the meaning of the CCPA.

For example, the Company collects and uses your personal information as appropriate to:

- Comply with applicable laws and regulations.
- Recruit and evaluate job applicants and candidates for employment.
- Conduct background checks.
- Engage clients for employment opportunities for job applicants and candidates.
- Manage your employment relationship with us, including for:
 - onboarding;
 - timekeeping, payroll, and expense reports;
 - employee benefits;
 - employee training and development;
 - the creation, maintenance, and security of your online employee accounts;
 - reaching your emergency contacts or beneficiaries when needed, such as when you are not reachable or are injured or ill;
 - workers' compensation claims management;
 - employee job performance, including goals and performance reviews, promotions, discipline, and termination; and
 - other human resources purposes.
- Manage and monitor employee access to company facilities, equipment, and systems.
- Conduct internal audits and workplace investigations.
- Investigate and enforce compliance with and potential violations of Company policies and procedures.
- Engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of the Company.
- Maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance.
- Perform workforce analytics, data analytics, and benchmarking.
- Administer and maintain the Company's operations, including for safety purposes.
- Market our services to clients and prospects.
- Exercise or defend the legal duties or rights of the Company and others, including its employees, affiliates, customers, contractors, service providers, and agents.

Retention Period for Personal Information

Pinnacle retains personal information for only as long as necessary to fulfill the purposes for the collection. Generally, personal information is retained for the duration of our employment relationship with you (or in the case of emergency contacts and beneficiaries, the employment relationship with the associated individual), plus any legally required record or data retention period and/or any period of time necessary to exercise our legal rights.

Your Privacy Rights

As a California resident, you have the following privacy rights regarding your personal information:

- The right to know and right to access the personal information we have collected about you, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom the business discloses personal information, and the specific pieces of personal information the business has collected about the consumer;
- The right to delete personal information that we have collected from you, subject to certain exceptions;
- The right to correct inaccurate personal information that we maintain about you;
- The right of portability, or right to have us transfer your personal information to other persons or entities upon your request;
- The right to limit the use of your sensitive information if we decide in the future to use such information for purposes other than the purposes listed above; and
- The right not to be discriminated against for exercising your of privacy rights.

You can exercise your privacy rights by submitting a request to us by emailing us at: privacy@pinnacle1.com calling us at: (214) 740-2424; or asking our Human Resources department for a written request form. To protect the security of your personal information, we will require you to provide us with identifying information for you such as personal email address, personal telephone number, employee identification number, and/or other information that we can match with the personal information we have collected about you to verify your identity.

You may use an authorized agent to request access to or deletion of your personal information. We will require your authorized agent to provide us with either (1) a power of attorney authorizing the authorized agent to act on your behalf or (2) your written authorization permitting the authorized agent to request access to your personal information on your behalf. Further, we will require you or your authorized agent to provide us with identifying information to verify your identity. We may also require you to either verify your own identity directly with us or directly confirm with us that you provided the authorized agent permission to submit the request.

Within ten (10) days of receiving your request to know, we will confirm receipt of your request and provide information about how we will process your request. Generally, we will respond to your request within forty-five (45) days. If we need more time to respond, we will provide you with notice and an explanation of the reason we need more time to respond. We may deny your request if we cannot verify your identity or are legally permitted to deny your request. If we deny your request, we will explain the basis for the denial, provide or delete any personal information that is not subject to the denial, and refrain from using the personal information retained for any purpose other than permitted by the denial. We will maintain a record of your request and our response for twenty-four (24) months.

Contact Information

This Notice is provided as a supplement to our full CPRA Privacy Policy for Work-Related Individuals (“Privacy Policy”) and is subject to all the terms of the Privacy Policy. To view the Privacy Policy, please visit <https://www.pinnacle1.com/privacy-policy/>.

If you have any questions about this Notice or need to access this Notice in an alternative format, please contact privacy@pinnacle1.com or (214) 740-2424.

Last Updated: December 29, 2022