

Dear Applicant,

Respecting the privacy of our employees is an essential part of our privacy program. We are committed to the proper handling of the Personal Information collected or processed in connection with your employment relationship with us. This disclosure describes the categories of Personal Information we collect and the purposes for which we process that information. In addition, the disclosure provides you with information on what rights you have with respect to the information collected by the Company.

California's California Consumer Privacy Act ("CCPA") and California Privacy Rights Act ("CPRA") provide California applicants and employees with certain rights:

- Knowledge of information collected;
- Deletion of information collected;
- Opt-out of information collected;
- Opt-in of information collected;
- Correction of information collected;
- Go to court;
- Limit use of information collected;
- Not to be discriminated or retaliated against for exercising rights under the CCPA and CPRA.

**Where We Get Your Information From.** The Company collects information about you from the following sources: 1) you; 2) prior employers, references, recruiters, job-related social media platforms; 3) third-party sources of demographic information; 4) third-party companies, such as background check companies, drug testing facilities; and 5) claim administrators and investigators. Depending on the Company's interactions with you, we may or may not collect all of the information identified about you.

**The Personal and Sensitive Personal Information That We Are Collecting.** We are collecting the following information:

- Identifiers, such as name, government-issued identifier (e.g., Social Security number), and unique identifiers (e.g., employee ID);

- Personal information, such as real name, signature, SSN, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, passport number, federal identification authorizing work in the United States, access and/or passcodes, insurance policy number, education, employment, employment history, bank account number, other financial information, medical information, or health insurance information;
- Characteristics of protected classifications under California or federal law, such as age, marital status, gender, sex, race, color, disability, citizenship, primary language, immigration status, military/veteran status, disability, request for leave, and medical conditions;
- Commercial information, such as transaction information and purchase history (e.g., in connection with travel or other reimbursements [or purchases from Company]);
- Internet or network activity information, such as browsing history and interactions with our online systems and websites and any personal information that you provide while accessing the Company's computer systems, such as personal credit card information and passwords;
- Geolocation data, such as device location from usage of the Company's devices
- Audio, electronic, visual, and similar information;
- Professional or employment-related information, such as work history and prior employer;
- Non-public education information; and
- Inferences drawn from any of the Personal and Sensitive Personal Information listed above to create a profile or summary about, for example, an individual's preferences and characteristics.

**How Your Personal and Sensitive Personal Information is Used.** We may use Personal and Sensitive Personal Information:

- To comply with state and federal law and regulations;
- To process payroll;
- To track time and attendance;
- To manage workers' compensation claims;
- To administer and maintain benefits, including group health insurance;
- To administer and maintain retirement service;

- To manage employee performance of their job duties, including promotions, discipline and/or termination;
- To conduct workplace investigations;
- To evaluate job applicants and candidates for employment;
- To obtain and verify background checks;
- To grant and monitor employees' access to secure company facilities;
- To implement, monitor, and manage electronic security measures on devices that are used to access networks and systems (e.g., incident management);
- To engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of the Company;
- To maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance;
- To anonymize and/or aggregate data to perform workforce analytics, data analytics, and benchmarking;
- To perform call monitoring and surveillance (e.g., CCTV); and
- Any other purposes authorized by the California Privacy Protection Agency, California or Federal law.

We may or may not have used Personal and Sensitive Personal Information about you for each of the above purposes.

**Sharing of Personal Information.** We only share your information with the following third-party entities: UKG and HireRight.

**Selling of Personal Information.** The Company DOES NOT sell your personal information.

**Data Retention.** The Company retains the information it receives about you for a period of: \_\_\_\_\_, unless a shorter or longer period is required by California or Federal law.

**For Inquiries and/or to Submit Requests for Information, Deletion or Correction.** Please contact Human Resources for inquiries about the Company's policy, or to submit your requests for