Privacy Policy for California Applicants and Employees

Cambridge-Lee Industries LLC (the "Company") is committed to protecting the privacy and security of personal information of its current and former California applicants and employees (collectively, "Employees" or "you") as well as your emergency contacts, dependents and beneficiaries in compliance with applicable law, including the California Consumer Privacy Act ("CCPA"). We collect information about you and your emergency contacts, dependents, and beneficiaries ("personal information") in connection with the Company's human resources, employment, benefits administration, health and safety, and business-related purposes, and to be in legal compliance as outlined in this Privacy Policy for California Employees ("Privacy Policy"). We do not sell or share, and in the past 12 months have not sold or shared personal information as defined under applicable law, including personal information of individuals we know to be under 16 years of age.

If you have any questions about this Privacy Policy or need access to this Privacy Policy in an alternative format for accessibility, please contact us by emailing Dennis Williams, Human Resource Manager, at DWilliams@camlee.com or calling 610.926.7379 (ext. 27379). This Privacy Policy may be updated from time to time to reflect changes in our personal information practices, and we will post a notice at the time of any such updates on intranet.camlee.com.

1. What Categories of Personal Information Do We Collect From Employees?

We collect, and within the past 12 months have collected, the following categories of personal information from our Employees, from devices used to access our IT systems, and through our service providers such as data analytics providers, social networks, identity verification and background screening, and benefits providers for the purposes described below:

A. Identifiers such as real name, initials or alias; postal address; unique personal identifiers such as or Employee ID; online identifiers such as IP address or online tracking ID; work or personal email address; account name, username, or other user ID; and forms of government identification such as Social Security Number, driver's license number, passport number, state ID number, national identity card details, or national identification number.

B. Additional types of information as described in California Civil Code § 1798.80(e) that may identify, relate to, describe, or be capable of being associated with particular individuals, including the "identifiers" listed in Subsection 1(A) and the following: date of birth or birthday; signature; physical characteristics or descriptions such as sensory information, including photographs as described in Subsection 1(G); information related to a protected class an Employee may be a part of as described in Subsection 1(C), vehicle information such as license plate number or vehicle registration information (e.g., color, make, or model); education information as described in Subsection 1(I); financial information, including gift card number, bank account information, bank account number, bank routing number, credit history, masked payment information, pensions, investment accounts, corporate credit card number, and any other financial information; insurance policy information such as insurance policy number; family information including Employee children's, spouse's, or parents' names

and emergency contact details; medical information such as height, weight, vaccine data, COVID 19 testing data, COVID 19 vaccination information, mental health status, disability status or specific condition, exercise data, and dietary data; online identifiers such as email, social media history, social media account, and social media contact information; and geolocation information as described in Subsection 1(F).

C. Characteristics of protected classifications under California or federal law such as race, color, religion, sex, gender, marital status, medical condition, mental health condition, disability status, national origin including nationality, residency, and citizenship status, sexual orientation; military and/or veteran status; requests for leave related to a family member's health, or an Employee health condition such as pregnancy; and age or age range (40 years and older).

D. Internet or other electronic network activity information, including but not limited to: IP address; online tracking ID; browsing history; search history; information regarding Employee interactions with an internet website or application; preferences related to digital communication; and information we collect (including through third-party suppliers) regarding content and other data posted on the Internet.

E. Geolocation data collected through apps, websites, or GPS-enabled devices or vehicles used in the context of employment.

F. Sensory information, including audio information such as voicemails or audio recordings; visual information such as photographs; or other similar information.

G. Professional or employment information, including: employment history; educational background and status as described in Subsection 1(I); qualifications; professional memberships and certifications; language capabilities; references, letters of recommendation and interview notes; areas of interest and work preferences; job preference, desired or expected salary, and work availability; relationship to Company; travel-related preferences, history, and details (e.g., known traveler number); information necessary for reimbursement, including corporate credit or debit card numbers and expense details; pre employment test results, including, reference checks, or background checks (based on the role); information provided by Employees during the candidacy and hiring process, including their completed application form; contract type, including whether an Employee is a temporary, fixed term, or permanent Employee; start date/orientation date, title/position, business unit/division, line or reporting manager, grade and department/organization and region/location of office; employment status, work-related contact details, date(s) of promotion, work history, and technical skills; training records; emergency contact information; compensation data, including salary, bonus, long-term incentives and award history; work time and payroll records, sick or vacation days used, records of work absences, vacation entitlement, annual leave, and requests; performance appraisals, disciplinary actions, grievances, complaints and related procedures; health and safety information and reporting; workers compensation claims; pensions, investment accounts, insurance and other benefits information and entitlements data (which may include information about an Employee's spouse,

children and other eligible dependents and beneficiaries); date of hire, date of resignation or termination, reason for resignation or termination, exit interview and comments, and other information relating to termination of employment; information collected in connection with taxation (such as information collected via standard tax forms) and verifying Employees' right to work in the United States (e.g., work authorization information), including information listed in Subsections 1(A), 1(B), and 1(C) above; and any information needed to comply with Company policies, EEOC or other reporting obligations, law, court or other governmental requests, or law enforcement authorities.

H. Education information defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99). This includes details contained in letters of application and resumes/CVs such as academic transcripts, education and training history, educational degrees, educational performance (e.g., grades received for coursework), and languages spoken.

I. Inferences drawn from any of the information identified in this subsection to create a profile about a person reflecting the person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

J. Sensitive personal information such as race, ethnicity, religion, Social Security Numbers, drivers' license number, state or national identification cards or numbers, passport number, account usernames and passwords, contents of any personal communications contained in Company emails, geolocation as described in Subsection 1(F), medical information and health insurance information as described in Subsection 1(B), financial information described in Subsection 1(B) under certain circumstances, and sexual orientation. However, we do not collect sensitive personal information for the purpose of inferring characteristics about Employees.

To the extent we or our third-party service and/or benefit providers collect additional categories of information beyond those described above, additional notice will be provided, and we or our third-party service and/or benefit providers will ask for Employee consent before collecting such additional categories of personal information, as required by law.

Personal information does not include information: (a) excluded from the scope of personal information under applicable law, (b) publicly available information or (c) de-identified or aggregate information. We maintain and use information in deidentified form, and we do not attempt to reidentify the information, except for the sole purpose of determining whether our deidentification processes satisfy the requirement under applicable law.

2. How Do We Use Employee Personal Information?

Personal Information collected from or about Employees is used for the following business purposes:

A. General Personal and Position Information, which may include name and contact information; Social Security number; driver's license number, vehicle information and tag number; passport and other government identification numbers; birth date; immigration and work authorization status; Employee photos; emergency contact information; household contact information; withholding tax and dependent information; voluntary self-disclosure information regarding race/ethnicity and gender; survey responses; any special needs during emergencies or travel; second languages; dietary and allergy information; employment status (full-time or part-time, regular, or temporary); education and work experience; job title, duties, and assignments; work schedule; hours worked and time off; accomplishments, certifications, and awards; business travel information; and expatriate and secondment assignments.

We collect and use this type of information to onboard new Employees, for training and development, to manage our employment relationships, and to comply with applicable laws. If required, the general personal and position information outlined in this section may also be used for purposes identified below and in accordance with applicable laws.

B. Pay and Expense Information such as pay rate, payroll deduction information, banking information for direct deposit (if applicable) and expense reimbursement, credit card information, and other expense reimbursement information.

We collect and use this type of information to pay and reimburse Employees and to comply with applicable laws.

C. Benefits Enrollment and Administration Information, which may include benefit selection information regarding benefits offered or sponsored by the Company such as retirement, life insurance, disability insurance, EAP, health insurance, and wellness programs; dependent and beneficiary information (including their contact information); leave of absence, disability status, and medical information; information you provide about yourself and your dependents and beneficiaries, as applicable, during the enrollment process; and other information necessary to administer benefits programs and process benefits claims.

We collect and use this type of information for enrollment in and administration of the Company's benefits for Employees and your dependents and beneficiaries, to provide reasonable accommodations and leaves of absence, and to comply with applicable laws.

D. Performance Management Information such as training and development information; performance evaluation information; discipline and counseling information; and employment termination information.

We collect and use this type of information to manage our employment relationship with Employees.

E. Health and Safety Information, which may include workplace testing, accident, illness, and injury information and related job restrictions; personal physician information (if applicable); and other health or related information to maintain a safe workplace, to assess your working capacity, to administer Workers' Compensation insurance programs, to comply with state and federal occupational safety and health regulations, standards and guidance, to comply with public health authority guidance, and to comply with applicable laws.

F. Workplace Security and Electronic Communications Information, which includes workplace video conferencing, recording, and security surveillance; electronic device usage such as email, computers, internet, telephones, and mobile devices; documents or other resources created on a Company device; IP addresses; log-in information; and location information.

We collect and use this type of information to protect the Company, customers, and Employee property, equipment, and confidential information; to monitor Employee performance; and to enforce the Company's policies, including the Employer Rights Regarding Employee Electronic Communications Systems Policy.

While relatively uncommon, there may be occasions when we use personal information of Employees for other purposes permitted under applicable law, for example, when are required to disclose information in connection with contractual or legal matters such as information necessary to respond to law enforcement and governmental agency requests (i.e., subpoenas); comply with legal and contractual obligations; exercise legal and contractual rights; and initiate or respond to legal claims.

We also use personal information of Employees for the following business purposes, where applicable, as described in applicable law: (1) helping to ensure security and integrity to the extent the use of the Employee's personal information is reasonably necessary and proportionate for these purposes; (2) debugging to identify and repair errors that impair existing intended functionality; (3) short-term, transient use, provided that the Employee's personal information is not disclosed to another third party and is not used to build a profile about the Employee or otherwise alter the Employee's experience outside the current interaction with the business; (4) performing services on behalf of the Company; (5) undertaking internal research for technological development and demonstration; and (6) undertaking activities to verify or maintain the quality or safety of a service or device that is owned by, manufactured by, manufactured for, or controlled by the Company, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the Company.

3. What Categories of Emergency Contact Information Do We Collect, and How Do We Use This Information?

We collect the following categories of personal information for the purposes described below:

A. Identifiers such as name and contact information; and

B. Additional types of information described in California Civil Code § 1798.80(e) such as relationship to the Employee.

We collect this information to contact the Employee's designated emergency contact persons in the event of an emergency.

4. What Categories of Dependent and Beneficiary Information Do We Collect, and How Do We Use This Information?

We collect the following categories of personal information of Employee dependents and beneficiaries for the purposes described below:

A. Identifiers such as name, contact information, and Social Security number; and

B. Additional types of information described in California Civil Code § 1798.80(e) such as birthday, relationship to Employee, and information necessary to process benefits claims.

We collect and use this information for enrollment in and administration of benefits programs for Employee dependents and beneficiaries.

5. How Do We Disclose Personal Information of Employees?

Some personal information, such as Employee contact information, may be disclosed to the Employees, independent contractors, or agents of the Company and our affiliates with access to payroll, performance management, benefits and other employment-related systems. Employee personal information may also be collected by or disclosed to IT service providers, performance management, travel agencies, and third-party service providers. We disclose, and in the past 12 months have disclosed, all categories of personal information we collect about Employees and their dependents and beneficiaries to these IT service providers, travel agencies, and third-party service providers so they can perform services on our behalf. In addition, we also disclose Employees' business contact information such as work email addresses, work phone numbers, and street addresses to our suppliers and business partners so they can contact our Employees and perform services on our behalf.

6. How Long Do We Retain Your Personal Information?

We retain and process Employee personal information for the length of time needed to carry out the purposes described in this Privacy Policy, and to the extent necessary to manage our relationships with Employees, comply with our legal obligations, resolve disputes, and enforce our agreements, consistent with our retention policy.

7. What Rights Do You Have Under California Privacy Law?

California residents have certain rights related to personal information, including:

A. The right to know the categories of personal information and/or the specific pieces of personal information we may hold about you.

B. The right to request that we delete personal information collected from you. However, please note that we may deny your deletion request as permitted under applicable law because we maintain and use personal information of Employees only for the length of time needed to carry out the purposes described in this Privacy Policy.

C. The right to request that we correct inaccurate personal information about you.

You may request to exercise these rights by emailing Dennis Williams, Human Resource Manager, at DWilliams@camlee.com or calling 610.926.7379 (ext. 27379).

Please note that we will take steps to verify your identity before granting you access to information or acting on your request to exercise your rights as required by applicable law. We may require you to provide your name, email address, street address, phone number, date of birth, last line reporting manager, and/or the last 4 digits of your Social Security number, as applicable, to verify your identity in response to exercising requests of the above type. We may limit our response to your exercise of the above rights as permitted under applicable law. When you submit a request to exercise your rights above, we will use the information you provide to process your request and to maintain a record of your request and our response, as permitted under applicable law.

We will confirm receipt of your request within ten (10) business days and endeavor to respond to a verifiable request within forty-five (45) days of the receipt of your request. If we need more time, we will inform you of the reason and extension period in writing.

8. How Can Your Authorized Agent Exercise Your Rights On Your Behalf?

You may designate an authorized agent to make a request on your behalf by emailing Dennis Williams, Human Resource Manager, at DWilliams@camlee.com or calling 610.926.7379 (ext. 27379). You may make such a designation by providing the agent with written permission to act on your behalf. We will require the agent to provide proof of that written permission. We may require you to verify your own identity in response to a request, even if you choose to use an agent, to the extent permitted by law.

9. Assurance of Non-Discrimination

You have the right to be free from discrimination by a business for exercising your CCPA privacy rights, including the right not to be retaliated against for exercising your CCPA privacy rights. We will not discriminate against you for exercising your CCPA privacy rights.