GELLERT
GLOBAL GROUP

FOR CALIFORNIA RESIDENTS

Employee and Applicant CCPA Notice

Last Updated: April 2023

This notice describes the categories of personal information collected by Atalanta Corporation and Camerican International, and all associated entities, ("Company") and the purposes for which such information may be collected and used. It also provides information concerning the Company's record retention practices and rights you may have under the CCPA.

We retain your personal information for as long as necessary to review your performance, provide pay and benefits, etc., and in accordance with the Company's data retention schedule. We may retain your personal information for longer if it is necessary to comply with our legal obligations or reporting obligations, resolve disputes, etc., or as permitted or required by applicable law. We may also retain your personal information in a deidentified or aggregated form so that it can no longer be associated with you. To determine the appropriate retention period for your personal information, we consider various factors such as the amount, nature, and sensitivity of your information; the potential risk of unauthorized access, use or disclosure; the purposes for which we collect or process your personal information; and applicable legal requirements. Personal Information does not include certain categories of information, such as publicly available information from government records, deidentified or aggregated consumer information, and information subject to HIPAA or the California Confidential Medical Information Act.

Categories of Personal Information Collected
Identifiers and Contact information. This category includes names, addresses, telephone numbers, mobile numbers, email addresses, signature, account name, dates of birth, bank account information, and other similar contact information and identifiers. Protected classification information. This category includes characteristics of protected classifications under California or federal law. Internet or other electronic network activity information. This category includes without limitation: • all activity on the Company's information systems, such as internet browsing history, search history, intranet activity, email communications, social media postings, stored documents and emails, usernames and passwords, and • all activity on communications systems including phone calls, call logs, voice mails, text messages, chat logs, app use, mobile browsing and search history, mobile email communications, and other information regarding an employee's use of company-issued devices. Geolocation data. This category includes GPS location data from the Company's information systems, including company-issued mobile devices and laptop computers. Audio, electronic, visual, thermal, olfactory, or similar information. This category includes, for example, information collected from camera, microphones, and similar devices. Biometric information. This category includes the use of biometric equipment, devices, or software to record

your time worked, to enter or exit facilities or rooms, to access or use equipment, or for other business purposes.

Professional and employment-related information. This category includes without limitation:

- data submitted with employment applications including salary history, employment history, employment recommendations, etc.,
- background check and criminal history,
- work authorization,
- fitness for duty data and reports,
- performance and disciplinary records,
- salary and bonus data,
- benefit plan enrollment, participation, and claims information, and
- leave of absence information including religious and family obligations, physical and mental health data concerning employee and his or her family members.

Education information. This category includes education history.

Limited medical information. This category includes without limitation:

- fitness for duty data and reports,
- leave of absence information including family obligations, physical and mental health data concerning employee and his or her family members.

Sensitive Personal Information. This category includes sensitive information such as

- social security, driver's license, state identification card, or passport number,
- financial account information that allows access to an account, including log-in credentials, financial account numbers, passwords, etc.,
- precise geolocation,
- racial or ethnic origin, religious or philosophical beliefs, or union membership,
- content of mail, email, and text messages unless the Company is the intended recipient of the communication,
- genetic data,
- biometric information for the purpose of uniquely identifying a consumer, and
- information concerning health, or sexual orientation, and related information.

Inferences drawn from the Applicant Personal Information in the categories above. This category includes engaging in human capital analytics, including but not limited to, identifying certain correlations about individuals and success on their jobs, analyzing data to improve retention, and analyzing employee preferences to inform HR Policies, Programs and Procedures.

Purposes Personal Information, Including Sensitive Personal Information, is Used

- Collect and process employment applications, including confirming eligibility for employment, background and related checks, onboarding, and related recruiting efforts.

- Processing payroll, other forms of compensation, and employee benefit plan and program design and administration including enrollment and claims handling, and leave of absence administration.

- To maintain physician records and occupational health programs.

- Maintaining personnel records and record retention requirements.
- Communicating with employees and/or employees' emergency contacts and plan beneficiaries.
- Complying with applicable state and federal health, labor, employment, benefits, workers compensation, disability, equal employment opportunity, workplace safety, and related laws, guidance, or recommendations.
- Preventing unauthorized access to, use, or disclosure/removal of the Company's property, including the Company's information systems, electronic devices, network, and data.
- Protect against fraud or other illegal activity or for risk management purposes.
- Ensuring and enhancing employee productivity and adherence to the Company's policies.
- To provide training and development opportunities.
- Investigating complaints, grievances, and suspected violations of Company policy.
- Design, implement, and promote the Company's diversity and inclusion programs.
- Facilitate the efficient and secure use of the Company's information systems.
- Ensure compliance with Company information systems policies and procedures.
- Improve safety of employees, customers and the public with regard to use of Company property and equipment.
- Improve efficiency, logistics, and supply chain management.
- Improve accuracy of time management systems, attendance, including vacations, sick leave and other absence monitoring.
- Evaluate an individual's appropriateness for a participation position at the Company, or promotion to a new position.
- Client engagement and other legitimate business purposes.
- To respond to and manage any legal claims against the Company and/or its personnel, including civil discovery in litigation.
- To facilitate other business administrative functions and strategic activities, such as risk management, information technology and communications, financial management and reporting, workforce and succession planning, mergers and acquisition activities; and maintenance of licenses, permits and authorization applicable to Company operations.

Sources of Personal Information We Collect

- **You**. We collect personal information from you during the course of your employment relationship with us. This includes personal information that you provide during your interactions with us, such as through our Site, by email, or when you communicate with us online, by phone, or at one of our locations. We also collect information through certain online tracking tools, such as browser cookies, flash cookies, and web beacons.

- **Related Entities and Affiliates**. We may collect information about you from our related parties and affiliates, including joint ventures.

- **Social media and related services**.

- **Service providers and contractors**. We may collect your PI from service providers and contractors who provide information about you that is needed as part of our employment administration activities, such as payroll and benefits administration.

- **News outlets, social media, surveys, and certain third parties**. In the course of performing our recruiting activities, we or third parties on our behalf may conduct research and other activities resulting in the collection of PI about you.

- **Information Collected Automatically**. As you navigate through and interact with our Site, we may compile statistical information concerning your usage of the Site through analytics services, such as those provided by Google Analytics. To do so, we may collect certain information about your equipment, browsing actions and patterns, including:
    - Details of your visits to our Site, such as traffic data, location data, logs and other communication data and the resources that you access and use on the Site
    - Information about your computer and internet connection, including your IP address, operating system, and browser type.
    - Information about the type of device you are using, mobile ad identifiers, the time and length of your visit, and the website that referred you to our Site.
    - Information about your preferences to make your use of the Site more productive, via the use of Cookies. For more information on Cookies, please see the Cookies and Other Tracking Technologies section. While all of this information can be associated with the IP address your computer had while you visited the Site, it will not be associated with you as an individual or with any other information you may submit through the Site or that we may store about you for any other purposes. We may use this information to generate aggregate statistics about visitors to our Site. Please check your web browser if you want to learn what information your browser sends or how to change your settings.

To carry out the purposes outlined above, the Company may disclose information with third parties or service providers, such as background check vendors, service providers such as information technology vendors, outside legal counsel, and state or federal governmental agencies.

We may also disclose your personal information if necessary to: (1) courts and government agencies to comply with federal, state, or local laws, as well as in connection with civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities; (2) law firms and their service providers to defend legal claims, (3) potential buyers or sellers of portions of our business in connection with due diligence related to organizational transactions.

The Company does not sell or share, as those terms are defined under applicable law, the above categories of Personal Information. We also do not use or disclose your sensitive personal information for purposes that, with limited exceptions, are not necessary to maintain the employment relationship as reasonably expected by an average employee. The Company may add to the categories of personal information it collects and the purposes it uses personal information. In that case, the Company will inform you.

California Resident Individual Rights Requests. Individuals who are residents of the State of California have certain individual rights as outlined below.

Upon receipt of a verifiable consumer request (see below), and as required by applicable law, we will provide a response to such requests.

Right To Know About Personal Information Collected or Disclosed. In addition to what is described above, as a California resident, you also have the right to request more information regarding the following topics , to the extent applicable:

- 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, if applicable,
- the categories of third parties to whom the business discloses personal information, and
- the specific pieces of personal information the business has collected about you.

Right To Request Deletion Of Your Personal Information. You have the right to request that we delete the personal information we collected or maintained about you. Once we receive your request, we will let you know what, if any, personal information we can delete from our records, and we will direct any service providers and contractors with whom we disclosed your personal information to also delete your personal information from their records.

There may be circumstances where we cannot delete your personal information or direct service providers or contractors to delete your personal information from their records. Such instances include, but are not limited to, enabling solely internal uses that are reasonably aligned with your expectations based on your relationship with the Company and compatible with the context in which you provided the information or to comply with a legal obligation.

Right to Request Correction. You have the right to request that the Company correct any inaccurate personal information we maintain about you, taking into account the nature of that information and purpose for processing it.

Right to Non-Discrimination for the Exercise of Your Privacy Rights. We will not discriminate or retaliate against you for exercising any of your rights as described above.

Submitting Consumer Rights Requests. To submit a California Consumer Rights request as outlined above, please contact the Company's Human Resources Department by calling us at **1-800-597-1172** or emailing us at **hr@gellertglobalgroup.com**. We reserve the right to only respond to verifiable consumer requests to know, delete, or correct.

A verifiable request is one made by any individual who is:

- the applicant who is the subject of the request,
- the authorized agent of the applicant.

What to submit. If we request, you must provide us with sufficient information to verify your identity and/or authority to act on behalf of the applicant. In general, we may ask you to provide identifying information that we already maintain about you or we may use a third-party verification service. In either event, we will try to avoid asking you for sensitive PI to verify your identity. We may not be able to respond to your request or provide you with PI if we cannot verify your identity or authority to make the request and confirm the PI relates to you. However, making a verifiable request does not require you to create an account with us.

Additionally, you will need to describe your request with sufficient detail to allow us to review, understand, assess, and respond. We will not use the PI we collect from an individual to determine a verifiable request for any other purpose, except as required or permitted by law.

Our response. We will endeavor to respond to a verifiable request within forty-five (45) calendar days of receipt, but we may require an extension of up to forty-five (45) additional calendar days to respond and we will notify you of the need for the extension.

If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option. The response we provide will also explain the reasons we cannot comply with a request, if applicable. To the extent permitted by the CCPA, we will respond to no more than two requests during any 12-month period.

Authorized Agent. You may authorize a natural person or a business (the Agent) to act on your behalf with respect to the rights under this section. When you submit a Request to Know, Correct, or Delete, the Agent must provide proof that you gave the Agent signed permission to submit the request, and you either must (i) verify you own identity with the business or (ii) directly confirm with us that you provide permission to the Agent. However, these steps are not required when you have provided the authorized agent with power of attorney pursuant to Probate Code sections 4000 to 4465. We reserve the right to deny requests from persons or businesses claiming to be authorized agents that do not submit sufficient proof of their authorization.

We reserve the right to amend this Notice at any time without advance notice. If you have questions about this notice, you may call **Human Resources, 1-800-597-1172.**