

## California Employee Privacy Policy

*Effective Date: December 9<sup>th</sup>, 2022*

Regional Management Corp. (“Regional Management,” “we,” “our,” or “us”) respects the privacy of our employee’s personal information.

Pursuant to the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (“CCPA”), we are required to provide California employees with a privacy policy that contains a comprehensive description of our online and offline practices regarding our collection, use, sale, sharing, and retention of their personal information as well as a description of the rights they have regarding their personal information. This Privacy Policy provides the information the CCPA requires as well as other useful information regarding our collection and use of personal information.

Please review this Privacy Policy carefully. From time to time, we may change this Privacy Policy. If we do, we will post an amended version on this webpage and on our intranet policy page (<https://regionalmanagement.sharepoint.com/>). You also may receive a copy by contacting us as described in the “**How to Contact Us**” section below.

This Privacy Policy covers the following topics:

- 1. Scope of Privacy Policy**
- 2. Notice at Collection of Personal Information**
- 3. Disclosure of Personal Information**
- 4. Retention of Personal Information**
- 5. Your Rights**
- 6. How to Submit a Request to Know, Delete, and/or Correct**
- 7. Our Process for Verifying a Request to Know, Delete, and/or Correct**
- 8. Other Relevant Policies, Including Monitoring**
- 9. Accessibility**
- 10. How to Contact Us**

## 1. Scope of Privacy Policy

### *When This Policy Applies*

This Privacy Policy is intended solely for, and is applicable only to, current and former California employees. Where relevant, it also applies to job applicants, interns, agency workers, contractors, consultants, directors, and other individuals whose information we collect in connection with providing employment. For ease of reference, this Privacy Policy generally refers to employee data, but this does not indicate in any way that an individual is our employee.

### *When This Policy Does Not Apply*

This Privacy Policy does not apply to individuals who are not California residents.

This Privacy Policy also does not apply to our collection and use of your personal information in a consumer or business-to-business capacity. For more information on our collection and use of your personal information in that capacity, including how we process opt-out preference signals, please see our online privacy policies available [here \(Regional Management\)](#) and [here \(Regional Finance\)](#) or at [https://s23.q4cdn.com/523605151/files/doc\\_downloads/2022/RMC-Investors-Privacy-Policy.pdf](https://s23.q4cdn.com/523605151/files/doc_downloads/2022/RMC-Investors-Privacy-Policy.pdf) (Regional Management) and <https://regionalfinance.com/site-privacy-policy/> (Regional Finance).

## 2. Notice at Collection of Personal Information

### *Personal Information We Collect*

The CCPA defines “personal information” to mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California resident or household. Personal information does not include publicly available, deidentified, or aggregated information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this Privacy Policy, we will refer to this information as “Personal Information.”

We currently collect and, in the 12 months prior to the Effective Date of this Privacy Policy, have collected the following categories of Personal Information from employees:

- Identifiers (name, postal address, online identifier, email address, account name, Social Security number, and driver’s license number)
- Unique personal identifiers (telephone numbers)
- Other type of state identification card number such as California ID Cards, or other states DMV office issued equivalent identification document number.
- Telephone number
- Signature
- Bank account number
- Other financial information, such as for example bank routing, number for direct deposits

- Insurance policy number or subscriber identification number
- Any unique identifier used by health insurer to identify employee
- Internet or other electronic network activity information (browsing history and search history)
- Commercial information, such as for example a commercial driver's license
- Education information
- Professional or employment-related information (including employment history)
- Characteristics of protected classifications under California or federal law (race, color, sex/gender (including pregnancy, childbirth, breastfeeding and/or related medical conditions), age (40 and older), national origin, disability (mental and physical, including HIV/AIDS, cancer, and genetic characteristics), citizenship status, genetic information, marital status, medical condition (genetic characteristics, cancer or a record or history of cancer), military or veteran status, request for family care leave, request for leave for an employee's own serious health condition, and request for pregnancy disability leave)
- Inferences drawn from above information to create a profile about an individual reflecting an individual's preferences, behavior, attitudes, intelligence, abilities, and aptitudes
- Sensitive Personal Information. Personal information that reveals an individual's social security number, driver's license, or state identification card; account name; or national origin; genetic data. Personal information collected and analyzed concerning an individual's health.

#### *Sources of Personal Information*

We collect Personal Information directly from California residents and from applicants, company insurers, benefits administrators, operating systems and platforms, background check service providers, recruiters, staffing companies, references, former employers, educational institutions, online providers (such as through LinkedIn and similar providers), government entities, other employees, business partners or coworkers, payroll providers, claims handlers. We do not collect all categories of Personal Information from each source.

#### *Purposes for Collection*

We currently collect and have collected the above categories of Personal Information for all purposes of providing employment, including to:

- To process payroll;
- To enable recruiting services;
- To have you fill out applications and forms associated with your employment or prospective employment;
- To perform background checks and drug testing;
- To verify your ability to work in this country;
- To identify you as a veteran;
- To have you acknowledge your agreement to certain company policies;
- To administer and maintain benefits, including group health insurance;
- To administer and maintain your retirement account;

- To administer and maintain compensation including bonuses;
- To administer and maintain leaves;
- To administer and maintain licensing for commercial selling of insurance products;
- To evaluate skills and preferences for additional work assignments;
- To administer and maintain your employment record;
- For emergency contact purposes;
- To track time and attendance at work;
- To manage workers' compensation claims;
- To manage your job-related performance;
- To grant and monitor your access to secure company facilities;
- To engage in corporate transactions requiring review of employee records and information such as for evaluating potential mergers and acquisitions;
- To maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance;
- To perform diversity and inclusion initiatives, including data analysis, development, and deployment;
- To investigate and handle disciplinary actions or termination;
- To establish training and/or development requirements;
- To detect fraud or other types of wrongdoing;
- To review web traffic and events, monitor for virus attacks and web content, and determine bandwidth consumption;
- To enforce our legal rights;
- Engage in other legitimate business purposes reasonably required for our day-to-day operations such as accounting, financial reporting, and business planning;
- To administer programs during a pandemic; and
- To comply with federal and state law.

We also use your Personal Information for the purposes described in our Team Member Handbook.

### 3. Disclosure of Personal Information

The following table identifies the categories of Personal Information that we disclosed for a business purpose in the 12 months preceding the Effective Date of this Privacy Policy and, for each category, the category of third parties to whom we disclosed Personal Information.

Categories of Personal Information	Categories of Third Parties
Personal identifiers (name, email address, postal address, telephone number, signature, Social Security Number, driver's license number, other type of state identification card number, bank account number, other similar identifiers)	Human resources platform services vendors; payroll/tax providers; government entities; benefit administrators; background check service providers; lawyers

Medical and insurance information (insurance policy number or subscriber identification number, any unique identifier used by health insurer to identify employee)	Human resources platform services vendors; company insurers; benefit administrators
Commercial information	Background check service providers, for example sharing a commercial driver's license number provided to us, for its validation.
Education, employment history, and related information	Background check service providers; recruiting software service vendors; licensing vendors; government entities; human resources platform services vendors; lawyers
Characteristics of protected classifications under California or federal law (race, color, sex/gender (including pregnancy, childbirth, breastfeeding and/or related medical conditions), age (40 and older), national origin, disability (mental and physical, including HIV/AIDS, cancer, and genetic characteristics), citizenship status, genetic information, marital status, medical condition (genetic characteristics, cancer or a record or history of cancer), military or veteran status, request for family care leave, request for leave for an employee's own serious health condition, and request for pregnancy disability leave)	Recruiting software service vendors; human resources platform services vendors; company insurers; benefit administrators; licensing vendors

We disclosed Personal Information to third parties for the following business or commercial purposes:

- To process payroll;
- To enable recruiting services;
- To perform background checks and drug testing;
- To verify your ability to work in this country;
- To administer and maintain benefits, including group health insurance;
- To administer and maintain licensing for commercial selling of insurance products;
- To manage workers' compensation claims;
- To maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance;
- To manage your job-related performance; and
- To comply with federal and state law.

We have not sold Personal Information in the twelve (12) months preceding the Effective Date of this Privacy Policy. We do not knowingly collect, sell, or share the Personal Information of individuals under 16 years of age. We do not use Sensitive Personal Information for purposes other than those allowed by the CCPA and its regulations.

#### **4. Retention of Personal Information**

We retain your Personal Information for as long as necessary to fulfill the purposes for which we collect it, such as to provide you with services you have requested, and for the purpose of satisfying any legal, accounting, contractual, or reporting requirements that apply to us.

#### **5. Your Rights**

If you are a California employee, you have the following rights with respect to your Personal Information:

- (1) The right to know what Personal Information we have collected about you, including the categories of Personal Information, the categories of sources from which we collected Personal Information, the business or commercial purpose for collecting, selling, or sharing Personal Information (if applicable), the categories of third parties to whom we disclose Personal Information (if applicable), and the specific pieces of Personal Information we collected about you;
- (2) The right to delete Personal Information that we collected from you, subject to certain exceptions;
- (3) The right to correct inaccurate Personal Information that we maintain about you;
- (4) If we sell or share Personal Information, the right to opt-out of the sale or sharing;
- (5) If we use or disclose sensitive Personal Information for purposes other than those allowed by the CCPA and its regulations, the right to limit our use or disclosure; and
- (6) The right not to receive discriminatory treatment by us for the exercise of privacy rights conferred by the CCPA.

#### **6. How to Submit a Request to Know, Delete, and/or Correct**

You may submit a request to know, delete, and/or correct through our interactive webform available [here](#), or by calling us toll-free at 1-833-708-4357.

If you are submitting a request on behalf of a California employee, please submit the request through one of the designated methods discussed above. After submitting the request, we will require additional information to verify your authority to act on behalf of the California employee.

In addition to the CCPA rights discussed above, California law provides current and former employees with the right to request certain information relating to their employment, such as the right to access their personnel file and payroll records. Because these requests are governed by laws that contain different requirements than the CCPA, we handle such requests separately from CCPA requests. If you would like to make such a request, please contact our Human Resources department by emailing [hr@regionalmanagement.com](mailto:hr@regionalmanagement.com).

If you would like to update your personal information, such as to notify us of a change of name or address, or if you have questions about your employment, please do so on Workday or contact our Human Resources department by emailing [hr@regionalmanagement.com](mailto:hr@regionalmanagement.com).

## **7. Our Process for Verifying a Request to Know, Delete, and/or Correct**

We will comply with your request upon verification of your identity and, to the extent applicable, the identity of the California employee on whose behalf you are making such request.

We will verify your identity either to a “reasonable degree of certainty” or a “reasonably high degree of certainty” depending on the sensitivity of the Personal Information and the risk of harm to you by unauthorized disclosure, deletion, or correction as applicable.

For requests to access categories of Personal Information and for requests to delete or correct Personal Information that is not sensitive and does not pose a risk of harm by unauthorized deletion or correction, we will verify your identity to a “reasonable degree of certainty” by verifying at least two data points that you previously provided to us and which we have determined to be reliable for the purpose of verifying identities.

For requests to access specific pieces of Personal Information or for requests to delete or correct Personal Information that is sensitive and poses a risk of harm by unauthorized deletion or correction, we will verify your identity to a “reasonably high degree of certainty” by verifying at least three pieces of Personal Information previously provided to us and which we have determined to be reliable for the purpose of verifying identities. In addition, you will be required to submit a signed declaration under penalty of perjury stating that you are the individual whose Personal Information is being requested.

## **8. Other Relevant Policies, Including Monitoring**

When we hire you, we provide you with other policies and procedures that govern your use of our offices, networks, computers, and other devices. We have the right to monitor your use of our offices and electronic resources in accordance with those policies and procedures.

You can find copies of these policies at our intranet (<https://regionalmanagement.sharepoint.com/>), or by contacting our Human Resources department by emailing to: [hr@regionalmanagement.com](mailto:hr@regionalmanagement.com).

## **9. Accessibility**

We are committed to ensuring this Privacy Policy is accessible to individuals with disabilities. If you wish to access to this Privacy Policy in an alternative format, please contact us as described below.

## **10. How to Contact Us**

To contact us for questions or concerns about this privacy policy or practices please contact us by us by emailing to: [hr@regionalmanagement.com](mailto:hr@regionalmanagement.com).