

**CALIFORNIA CONSUMER PRIVACY ACT (CCPA) NOTICE AT COLLECTION:
APPLICANTS, EMPLOYEES, and WORKFORCE MEMBERS**

Last Updated: February 1, 2024

This Notice at Collection (“Notice”) describes the categories of Personal Information that Milliken and Company (“Company”) collects from and about California applicants, employees, and workforce members the purposes for which the Company collects and uses such information, how long we retain this information, and rights you may have under the California Consumer Privacy Act (“CCPA”).

For additional information about the Company’s data privacy practices, please review information contained at <https://www.milliken.com/en-us/privacy>.

Categories of Personal Information
<p>We May Collect, or Have Collected in the Past 12 Months, the following categories of Personal Information:</p> <p><u>Identifiers and Contact information.</u> This category includes names, addresses, telephone numbers, mobile numbers, email addresses, signatures, account names, dates of birth, bank account information, and other similar contact information and identifiers.</p> <p><u>Protected Classification Information.</u> This category includes characteristics of protected classifications under California or federal law.</p> <p><u>Internet or Other Electronic Network Activity Information.</u> This category includes, without limitation:</p> <ul style="list-style-type: none">• all activity on the Company’s information systems, such as internet browsing history, search history, intranet activity, email communications, stored documents and emails, usernames and passwords• all activity on communications systems, including phone calls, call logs, voice mails, text messages, chat logs, app use, and search history, mobile email communications, and other information regarding an employee’s use of company-issued devices. <p><u>Geolocation Data.</u> This category includes, without limitation, GPS location data from the Company’s information systems, company-owned or issued mobile devices, applications, or vehicles.</p> <p><u>Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information.</u> This category includes, for example, information collected from cameras, and similar devices.</p> <p><u>Biometric Information.</u> This category includes the use of biometric equipment, devices, or software to establish individual identity, record your time worked, to enter or exit facilities or rooms, to access or use equipment or for other business purposes, and for certain wellness metrics.</p> <p><u>Professional and Employment-Related Information.</u> This category includes without limitation, where permitted by law:</p>

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

Education Information. This category includes, without limitation, education history.

Sensitive Personal Information. This category includes, without limitation:

- 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)
- biometric information for the purpose of uniquely identifying a consumer
- genetic or health information
- information concerning health and sex life or sexual orientation.

Inferences Drawn from the Personal Information in the Categories Above. This category includes engaging in human capital analytics, including, without limitation, identifying correlations between certain characteristics and job success, analyzing data to improve retention, and analyzing employee preferences to inform HR policies, programs, and procedures.

Purposes for Which Personal Information Is Used

Where applicable, and permitted by law, we may use your Personal Information for the following purposes:

- Collecting and processing employment applications, including confirming eligibility for employment, background and related checks, drug tests, references, onboarding, and related recruiting efforts.

- Maintaining physician records and occupational health programs.
- Maintaining records and satisfying record retention requirements.
- Communicating with applicants about a current application, future job opportunities or current and past employment
- Submitting relevant information to prospective employers.
- Submitting relevant information for payment of wages and bonuses.
- Complying with applicable state and federal health, labor, employment, 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.
- 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.
- Communicating with employees and/or employees' emergency contacts and plan beneficiaries.
- Ensuring and enhancing employee productivity and adherence to the Company's policies.
- Improving accuracy of time management systems, attendance, including vacations, sick leave and other absence monitoring.
- Providing training and development opportunities.
- Investigating complaints, grievances, and suspected violations of Company policy.
- Designing, implementing, and promoting the Company's diversity and inclusion programs.
- Facilitating the efficient and secure use of the Company's information systems.
- Ensuring compliance with the Company information systems policies and procedures.
- Improving safety of applicants, employees, customers and the public with regard to use of Company property and equipment.
- Improving efficiency.
- Evaluating an individual's appropriateness for a particular position at the Company or promotion to a new position.
- Protecting the legal rights, privacy, safety or property of Company or its employees, agents, contractors, customers or the public.
- Protecting against fraud or other illegal activity or for risk management purposes.
- Responding to and managing legal claims against the Company and/or its personnel, including civil discovery in litigation.
- Facilitating other business administrative functions and strategic activities, such as risk management, information technology and communications, financial management and reporting, workforce and succession planning, merger and acquisition activities, and maintenance of licenses, permits and authorization applicable to Company operations.

Sources of Personal Information

We may collect your Personal Information from the following sources:

- *You.* We may collect Personal Information directly from you or your device, such as through your use of our website, facilities or systems, when you send us an email, contact us by phone, or otherwise communicate or interact with us. We collect information when you are an applicant for employment with us or employed by us.
- *Related Entities and Affiliates.* We may collect information about you from our related parties and affiliates.
- *Social media and related services.* We may collect information about you through your social media services consistent with your settings on such services.
- *Third parties.* We may collect information about you from third parties such as your references, background check vendors, staffing agencies, clients, or other third-party sources that are lawfully entitled to share your data with us. This may include service providers or contractors who collect or process your PI on our behalf.

Disclosure of Your Personal Information

To carry out the purposes outlined above, we may disclose, or have disclosed in the past 12 months, your Personal Information to our affiliates, service providers and contractors (e.g., background check vendors, third-party staffing vendors, payroll processors, information technology vendors), outside legal counsel and government entities.

We may also disclose your personal information to additional parties, if necessary, to: (1) comply with federal, state, or local laws; (2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities; (3) cooperate with law enforcement agencies concerning conduct or activity that we reasonably and in good faith believe may violate federal, state, or local laws; or (4) exercise or defend legal claims.

Lastly, we may transfer Personal Information to a third party as part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control or acquires of all or part of the assets of our business.

Categories of Personal Information	Example Categories of Third Parties to Whom Personal Information May be Disclosed
Address and other identifiers – such as name, postal address, email address, phone number, account name, date of birth, Social Security number, driver’s license number, photograph, passport number, unique personal identifier, online identifier, Internet Protocol address, email	Third parties as directed by you. Affiliates. Our business partners.

<p>address, account name, or other similar identifiers</p> <p>NOTE: The information in this category may include the following elements of Sensitive Personal Information: Social Security number, driver’s license number, state identification card number, and/or passport number.</p>	<p>Our clients or customers.</p> <p>Your union.</p> <p>Third parties that perform services on our behalf. For example, we may disclose information to certain service providers, information technology providers, payroll and benefits managers, and data storage companies. We might also authorize our service providers to collect personal information on our behalf.</p> <p>Successors to all or portions of our business. If all or part of our business is sold or merged, we may disclose personal information in preparation for or as part of that transaction.</p> <p>Governmental entities, legal service providers.</p>
<p>Protected status – such as citizenship, ethnic background, gender, or other similar identifiers</p> <p>NOTE: The information in this category may include the following elements of Sensitive Personal Information: racial, ethnic, or national origin.</p>	<p>Third parties as directed by you.</p> <p>Affiliates.</p> <p>Your union.</p> <p>Third parties that perform services on our behalf. For example, we may disclose information to certain service providers, information technology providers, payroll and benefits managers, and data storage companies. We might also authorize our service providers to collect personal information on our behalf.</p> <p>Successors to all or portions of our business. If all or part of our business is sold or merged, we may disclose personal information in preparation for or as part of that transaction.</p> <p>Governmental entities, legal service providers</p>
<p>Financial information – such as bank account details, credit history, income details or other similar identifiers</p> <p>NOTE: The information in this category may include the following elements of Sensitive Personal Information: log-in, financial account in combination with any required security or access code, password, or credential allowing access to an account.</p>	<p>Third parties as directed by you.</p> <p>Affiliates.</p> <p>Your union.</p> <p>Third parties that perform services on our behalf. For example, we may disclose information to certain service providers, information technology providers, payroll and benefits managers, and data storage companies. We might also authorize</p>

	<p>our service providers to collect personal information on our behalf.</p> <p>Successors to all or portions of our business. If all or part of our business is sold or merged, we may disclose personal information in preparation for or as part of that transaction.</p> <p>Governmental entities, legal service providers</p>
<p>Commercial information – such as records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies or other similar identifiers</p>	<p>Third parties as directed by you.</p> <p>Affiliates.</p> <p>Your union.</p> <p>Third parties that perform services on our behalf. For example, we may disclose information to certain service providers, information technology providers, payroll and benefits managers, and data storage companies. We might also authorize our service providers to collect personal information on our behalf.</p> <p>Successors to all or portions of our business. If all or part of our business is sold or merged, we may disclose personal information in preparation for or as part of that transaction.</p> <p>Governmental entities, legal service providers.</p>
<p>Education or professional information, including veteran status or other similar identifiers</p> <p>NOTE: The information in this category may include the following elements of Sensitive Personal Information: union membership.</p>	<p>Third parties as directed by you.</p> <p>Affiliates.</p> <p>Your union.</p> <p>Third parties that perform services on our behalf. For example, we may disclose information to certain service providers, information technology providers, payroll and benefits managers, and data storage companies. We might also authorize our service providers to collect personal information on our behalf.</p> <p>Successors to all or portions of our business. If all or part of our business is sold or merged, we may disclose personal information in preparation for or as part of that transaction.</p> <p>Governmental entities, legal service providers</p>

<p>Internet or other electronic network activity – such as browsing history, search history, a consumer’s interaction with an internet website, application, or advertisement</p> <p>NOTE: The information in this category may include the following elements of Sensitive Personal Information: the contents of mail, email, or text messages, to which the business was not the intended recipient.</p>	<p>Third parties as directed by you.</p> <p>Affiliates.</p> <p>Your union.</p> <p>Third parties that perform services on our behalf. For example, we may disclose information to certain service providers, information technology providers, payroll and benefits managers, and data storage companies. We might also authorize our service providers to collect personal information on our behalf.</p> <p>Successors to all or portions of our business. If all or part of our business is sold or merged, we may disclose personal information in preparation for or as part of that transaction.</p> <p>Governmental entities, legal service providers</p>
<p>Geolocation data</p> <p>NOTE: The information in this category may include the following elements of Sensitive Personal Information: precise geolocation.</p>	<p>Third parties as directed by you.</p> <p>Affiliates.</p> <p>Your union.</p> <p>Third parties that perform services on our behalf. For example, we may disclose information to certain service providers, information technology providers, payroll and benefits managers, and data storage companies. We might also authorize our service providers to collect personal information on our behalf.</p> <p>Successors to all or portions of our business. If all or part of our business is sold or merged, we may disclose personal information in preparation for or as part of that transaction.</p> <p>Governmental entities, legal service providers</p>
<p>Audio, electronic, visual or similar information.</p>	<p>Third parties as directed by you.</p> <p>Affiliates.</p> <p>Your union.</p> <p>Third parties that perform services on our behalf. For example, we may disclose information to certain service providers, information technology providers, payroll and benefits managers, and</p>

	<p>data storage companies. We might also authorize our service providers to collect personal information on our behalf.</p> <p>Successors to all or portions of our business. If all or part of our business is sold or merged, we may disclose personal information in preparation for or as part of that transaction.</p> <p>Governmental entities, legal service providers</p>
<p>Biometric Information</p> <p>NOTE: Biometric information is considered an element of Sensitive Personal Information.</p>	<p>Third parties as directed by you.</p> <p>Affiliates.</p> <p>Your union.</p> <p>Third parties that perform services on our behalf. For example, we may disclose information to certain service providers, information technology providers, payroll and benefits managers, and data storage companies. We might also authorize our service providers to collect personal information on our behalf.</p> <p>Successors to all or portions of our business. If all or part of our business is sold or merged, we may disclose personal information in preparation for or as part of that transaction.</p> <p>Governmental entities, legal service providers</p>
<p>Inferences drawn from personal information – such as individual profiles, preferences, characteristics, behaviors or other similar identifiers</p> <p>NOTE: The information in this category may include the following elements of Sensitive Personal Information: racial or ethnic origin, religious or philosophical beliefs, union membership, health information.</p>	<p>Third parties as directed by you.</p> <p>Affiliates.</p> <p>Your union.</p> <p>Third parties that perform services on our behalf. For example, we may disclose information to certain service providers, information technology providers, payroll and benefits managers, and data storage companies. We might also authorize our service providers to collect personal information on our behalf.</p> <p>Successors to all or portions of our business. If all or part of our business is sold or merged, we may disclose personal information in preparation for or as part of that transaction.</p> <p>Governmental entities, legal service providers</p>

The Company may add to the categories of Personal Information we collect and how we use your information. In that case, the Company will inform you.

We do not sell or share, as those terms are defined under the CCPA, the above categories of Personal Information.

We do not use or disclose your Sensitive Personal Information for purposes that, with limited exceptions, are not necessary for the application or employment related purpose for which we collect it, as reasonably expected by an average individual in this context, for other permitted purposes under the CCPA, or as authorized by regulation.

Retention. We retain your Personal Information for as long as is necessary to fulfill the purpose for which it was collected (e.g., to process your application for employment, manage the employment relationship, 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 or reporting obligations (e.g., if we are required to retain your data to comply with applicable laws), resolve disputes, enforce our legal agreements and policies, address other legitimate business needs, 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, and deidentified or aggregated information.

California Resident Individual Rights Requests. Individuals who are residents of the State of California have the following rights, subject to certain limitations.

Right To Know About Personal Information Collected or Disclosed. As a California resident, you have the right to request additional information beyond what we disclosed above regarding the following, to the extent applicable:

- the categories of Personal Information the Company collected about you
- the categories of sources from which that Personal Information was collected
- the business or commercial purposes for which that information was collected, sold, or shared
- the categories of third parties to whom the information was disclosed
- the specific pieces of Personal Information collected

Upon receipt of a verifiable Request to Know and as required by applicable law, we will provide a response to such a request.

Right To Request Deletion of Your Personal Information. You have the right to request that we delete the Personal Information we collected or maintain about you. Once we receive your request, we will let you know what, if any, Personal Information we can delete from our records and will direct any service providers, contractors, and third parties to 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, contractors, or third parties to delete your Personal Information from their records. Without limitation, such instances include when the information is maintained: (a) to enable solely internal uses that are reasonably aligned with your expectations based on your relationship with us and compatible with the context in which you provided the information, or (b) to comply with a legal obligation.

Upon receipt of a verifiable Request to Delete, and as required by applicable law, we will provide a response to such requests.

Right to Request Correction. You have the right to request that we correct any inaccurate Personal Information we maintain about you, taking into account the nature of that information and the purpose for processing it. Upon receipt of a verifiable Request to Correct and as required by the CCPA, we will provide a response to such requests.

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

Submitting CCPA Rights Requests. To submit a CCPA Rights request, please contact us at 888.553.1213 or email us at privacy@milliken.com. We reserve the right to only respond to *verifiable* Requests to Know, Delete, or Correct that are submitted as instructed.

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

- the subject of the request,
- acting on behalf of their minor child, or
- the authorized agent of the individual.

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 individual. 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 Personal Information to verify your identity. We may not be able to respond to your request or provide you with Personal Information if we cannot verify your identity or authority to make the request and confirm the Personal Information 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 Personal Information we collect from an individual to determine a verifiable request for any other purpose, except as required or permitted by law.

Our response. We reserve the right to charge a fee to process or respond to your request if it is excessive, repetitive, or manifestly unfounded. If we determine that a request warrants a fee, we will attempt to notify you as to why we made that decision and provide a cost estimate before completing your request. 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.

Authorized Agent. You may authorize a natural person or a business (the Agent) to act on your behalf. 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.

Spouses, Dependents, and Associates. If you have knowledge that the Company collected Personal Information related to your spouse or dependent, please share a copy of this notice with all such individuals.

Updates. We reserve the right to amend this notice. Please direct questions about this notice to privacy@milliken.com.