

California Employee Privacy Policy

Effective Date: October 1, 2025

Duraflame, Inc. (“Duraflame,” “we,” “our,” or “us”) respects the privacy of our employees’ 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. 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:

- Scope of Privacy Policy
- Notice at Collection of Personal Information
- Disclosure of Personal Information
- Retention of Personal Information
- Your Rights
- How to Submit a Request to Know, Delete, and/or Correct
- Our Process for Verifying a Request to Know, Delete, and/or Correct
- Other Relevant Policies, Including Monitoring
- Accessibility
- 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 policy available here at <https://duraflame.com> [www.duraflame.com/terms-of-use#PrivacyPolicy](https://duraflame.com/terms-of-use#PrivacyPolicy).

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, alias, postal address, online identifier, email address, Social Security number, driver’s license number, and other similar identifiers)
- Unique personal identifiers (device identifier; cookies, beacons, pixel tags, mobile ad identifiers, or other similar technology; unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular candidate or employee)
- Other types of state identification card numbers such as California ID cards
- Telephone number
- Signature
- Physical characteristics or description
- Bank account number
- Corporate credit card number
- Medical information
- Insurance policy number or subscriber identification number
- Any unique identifier used by health insurers to identify consumer
- Any information in an individual’s application and claims history, including appeals records, if information is linked or reasonably linkable to an individual or household, including via device, by business or service provider
- Internet or other electronic network activity information (information regarding an individual’s interaction with website or application)
- Geolocation data (regional, city/state, and precise)
- Records of personal property
- Education information
- Professional or employment-related information (including employment history, requests for leave under our leave policies)
- Biometric information (fingerprint, imagery of face, imagery of hand, imagery of palm, voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, keystroke patterns or rhythms, and gait patterns or rhythms)

- Characteristics of protected classifications under California or federal law (race, color, sex/gender (including pregnancy, childbirth, breastfeeding and/or related medical conditions), sexual orientation, gender identity/expression, age (40 and older), national origin, ancestry, disability (mental and physical, including HIV/AIDS, cancer, and genetic characteristics), citizenship or immigration status, genetic information, marital status, medical condition (genetic characteristics, cancer or a record or history of cancer), military or veteran status, status as a victim of domestic violence, assault, or stalking, requests for family care leave, an employee's own serious health condition, and pregnancy disability leave)
- Audio, video, electronic, thermal, or similar information (e.g., CCTV video footage, temperature screenings)
- Inferences drawn from above information to create a profile about an individual reflecting an individual's preferences and/or characteristics

Sources of Personal Information

We collect Personal Information directly from you (California residents) and from recruiters; staffing companies; references; former employers; educational institutions; online providers (such as through LinkedIn and similar providers); government entities; other employees; business partners; payroll providers; benefits providers; medical providers; background checks; company bankers; claims handlers; authentication and single sign-on providers; advertising networks; internet service providers; data analytics providers; operating systems, platforms, or software; social networks; data brokers; and surveillance systems. 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:

- Process payroll;
- Request your complete applications and forms associated with your employment or prospective employment;
- Consider you for potential employment;
- Perform a background check;
- Verify your ability to work in this country;
- Identify you as a veteran;
- Process security clearances;
- Perform diversity and inclusion initiatives, including data analysis, development and deployment;
- Request you acknowledge your agreement to certain company policies;
- Enroll you in our wellness program;
- Administer and maintain benefits, including group health insurance;
- Administer and maintain your retirement account;
- Contact individuals for emergency purposes;
- Track time and attendance at work;
- Manage workers' compensation claims;

- Manage your job-related performance;
- Arrange business travel;
- Investigate and handle disciplinary actions or termination;
- Establish training and/or development requirements;
- Detect fraud or other types of wrongdoing;
- Grant and monitor your access to secure company facilities;
- Engage in corporate transactions requiring review of employee records and information, such as for evaluating potential mergers and acquisitions;
- Review web traffic and events, monitor for virus attacks and web content, and determine bandwidth consumption;
- Maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance;
- Prevent the spread of COVID-19;
- Perform call monitoring and surveillance (e.g., CCTV);
- Comply with federal and state law;
- Enforce our legal rights; and
- Engage in other legitimate business purposes reasonably required for our day-to-day operations such as accounting, financial reporting and business planning.

We also use your Personal Information for the purposes described in our Employee Handbook, Acceptable Use Policy, Workplace Monitoring Policy, and, to the extent applicable, our Attendance Policy.

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 categories of recipients to whom we disclosed Personal Information.

Categories of Personal Information	Categories of Recipients
Personal identifiers (name; alias; postal address; online identifier; email address; Social Security number; driver's license number; device identifier; cookies, beacons, pixel tags, mobile ad identifiers, or other similar technology; unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular candidate or employee; other types of state identification card numbers; telephone number; signature; physical characteristics or description; bank account number; corporate credit card number; information regarding an individual's interaction with website or application; geolocation data; records of personal property)	Human resource information systems; operating systems and platforms; customer relationship management systems; background check service providers; government or law enforcement entities; applicant and recruiter software; payroll/tax providers; expense management service providers; enterprise travel providers; data analytics providers; company bankers; authentication and single sign-on providers; security providers; mobile device management providers; accountants; lawyers; benefits providers; social networks; company insurers; communication service providers; training service providers; consultants and other professional advisors

Medical and insurance information (medical information; insurance policy number or subscriber identification number; any unique identifier used by health insurer to identify consumer; any information in an individual's application and claims history, including appeals records, if information is linked or reasonably linkable to an individual or household, including via device, by business or service provider)	Benefits providers; company insurers; professional employer organizations; human resource information systems; communication service providers; lawyers; government or law enforcement entities
Education, employment history, and related information	Applicant and recruiter software; professional employer organizations; human resource information systems; payroll/tax providers; background check service providers; benefits providers; lawyers; government or law enforcement entities
Biometric information (fingerprint, imagery of face, imagery of hand, imagery of palm, voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, keystroke patterns or rhythms, and gait patterns or rhythms)	Human resource information systems; badge and security providers; operating systems and platforms; background check service providers; government or law enforcement entities; applicant and recruiter software; payroll/tax providers; data analytics providers; authentication and single sign-on providers; mobile device management providers; benefits providers; company insurers; communication service providers; consultants and other professional advisors
Characteristics of protected classifications under California or federal law (race; color; sex/gender (including pregnancy, childbirth, breastfeeding and/or related medical conditions); sexual orientation; gender identity/expression; age (40 and older); national origin; ancestry; disability (mental and physical, including HIV/AIDS, cancer, and genetic characteristics); citizenship or immigration status; genetic information; marital status; medical condition (genetic characteristics, cancer or a record or history of cancer); military or veteran status; status as a victim of domestic violence, assault, or stalking; requests for family care leave, an employee's own serious health condition, and pregnancy disability leave)	Applicant and recruiter software; professional employer organizations; government or law enforcement entities; human resource information systems; benefits providers; payroll/tax providers; company insurers; background check service providers; lawyers
Audio, video, electronic, thermal, or similar information (e.g., CCTV video footage, temperature screenings)	Human resource information systems; badge and security providers; operating systems and platforms; background check service providers; government or law enforcement entities; applicant and recruiter software; payroll/tax providers; data analytics providers; authentication and single sign-on providers; mobile device management providers; communication service providers; training service providers; consultants and other professional advisors

We disclosed Personal Information to the above categories of recipients for all of the business or commercial purposes identified in the above “Purposes for Collection” section.

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 collect or process Personal Information for the purpose of inferring characteristics.

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. Please contact us as described in the “How to Contact Us” section below for more information on our employee data retention schedule.

5. Your Rights

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

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;

- The right to delete Personal Information that we collected from you, subject to certain exceptions;
- The right to correct inaccurate Personal Information that we maintain about you;
- If we sell or share Personal Information, the right to opt-out of the sale or sharing;
- 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
- 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 by emailing us at

<https://www.duraflame.com/contact-us/> or by mail at 2879 Saint Rose Parkway, Henderson, NV 89052.

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 submit your request through <https://www.duraflame.com/contact-us/>.

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 submit your request or question through <https://www.duraflame.com/contact-us/>.

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 may 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.

For more information, please read our Employee Handbook. You can request a copy by contacting your local work location.

9. Accessibility

We are committed to ensuring this Privacy Policy is accessible to individuals with disabilities. If you wish to access 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 our privacy policies or practices please visit <https://www.duraflame.com/contact-us/>.