Applicant Privacy Notice

Effective date December 01, 2025

This Applicant Privacy Notice explains how GAF Materials LLC d/b/a GAF, GAF Canada ULC, GAF Energy LLC, and their direct and indirect subsidiaries that do not maintain their own privacy policy (collectively, "Company", "we", "us", or "our") handles the personal data of applicants, contingent workers and independent contractors ("You").[1] Personal data includes information that identifies you, and other information that relates to you and can be associated with you.

The "Systems Monitoring" section of this Notice (Section 3) details how the Company monitors, records, and analyzes (i) data about Your use of Company-issued devices, media, applications, network resources and IT services, and third-party services contracted by the Company (collectively "**IT Assets**"), and (ii) data or communications transmitted to or from, printed from, or created, stored, recorded or accessed on IT Assets.

This Applicant Privacy Notice is designed to meet obligations under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (together, the "CCPA"). In the event of a conflict between any other policy, statement, or notice and this Applicant Privacy Notice, this Applicant Privacy Notice will prevail as to California job applicants, unless stated otherwise. This Applicant Privacy Notice does not apply to our consumer facing website(s), which are addressed in our general privacy policy available here, except when you submit a job application to us. It also does not apply to our current or former employees or independent contractors.

1. Personal Data We Hold About You

The Company receives personal data from and about You in the course of managing the potential working relationship. You will provide much of this data directly to the Company, and personal data that is not provided directly by You will either be generated about You by the Company or obtained from other sources (e.g., from recruiting agencies, consumer reporting agencies, former employers, academic institutions, or publicly available resources).

The personal data we handle about You includes:

- identifiers (e.g., legal name, preferred name or nickname, date of birth, home address, personal email address, phone number, social security number, driver's

[1] The use of the term "Personnel" in this Notice does not and should not be interpreted as conveying any benefits or rights, or change of employment or engagement status different from that previously agreed to by the Company.

license number, passport number, documents supporting immigration status and right to work, device identifiers such as IP addresses and cookies);

- protected characteristics, such as gender, age, race, sexual orientation and other diversity and equal opportunity information we collect on a voluntary basis to comply with federal law;

- education information (e.g., education history, qualifications, certifications, academic records, training undertaken, and training needs);

- professional or employment-related information (e.g., resumes, employment history, job title, department, job responsibilities, manager/supervisor name, employment status, professional memberships, work location, office address, union membership, compensation and benefits, expenses, information provided to process expenses, information about your performance or conduct from other personnel, clients or service providers you worked with at a prior Company, who may provide feedback about you for reference checking purposes);

- background check information from private employment screening agencies, consumer reporting agencies, or publicly available registers, and drug and alcohol test results from private screening companies, police reports, or medical institutions;

- references obtained during recruitment from your former employers, educational institutions, individuals or organizations you identify as references, and organizations with which you are affiliated or from which you hold certifications or similar qualifications;

- publicly available professional profiles on privately owned websites or social media platforms (e.g., LinkedIn) where your profiles are displayed for networking and similar purposes;

- biometric information within the meaning of the California Consumer Privacy Act ("CCPA")(e.g., fingerprints, optional facial recognition);

- communications;

- audio, electronic, visual, thermal, olfactory, or similar information (e.g., photographs, CCTV or other video surveillance at Company property, voicemails, recording of meetings);

- internet or other electronic network activity information (e.g., communications, browsing history, search history, interactions with websites and applications, and other usage of Company electronic resources or technology);

- other data about use of IT Assets and any data or communications transmitted to or from, printed from, or created, stored, recorded or accessed on any of the above (see the “Systems Monitoring” section below for more detail);

- precise geolocation data (e.g. company vehicle location); and

- inferences drawn from any of the information identified in this Notice.

Some of the information we collect is covered by California Civil Code Section 1798.80(e) and local law.

2. Purposes of Processing

The Company will process personal data in order to manage our potential working relationship with You. In general, this is to comply with the Company’s legal obligations to You, to manage its records, to comply with applicable law, and to ensure its business functions properly. In particular, the Company processes personal data for the purposes of:

- managing the potential working relationship (e.g., recruitment and headcount management, training, career and professional development and talent management, administration of Your records and business travel);

- conducting criminal background checks and drug and alcohol testing, to the extent that these are permitted by applicable law;

- protecting intellectual property, confidential information, and our assets;

- monitoring the security of our facilities and Company systems;

- planning changes in group structure, security management, and record-keeping purposes;

- compliance with legal and regulatory obligations related to employment, media, data protection, and other applicable laws and regulations;

- handling legal claims and disputes;

- creating aggregated or de-identified personal data, which we may use for any purpose; and

- otherwise operating our business.

Consistent with applicable law, we may use personal data with artificial intelligence tools to assist us in various HR functions, such as recruiting, hiring, firing, discipline, or

determining the terms or conditions of employment.

3. Systems Monitoring

For lawful security and business management purposes, the Company may monitor, record and analyze:

- data about any of Your use of any Company-issued devices, media, applications, network resources and IT services, and third-party services contracted by the Company (collectively, "**IT Assets**"); and

- any data or communications transmitted to or from, printed from, or created, stored, recorded or accessed on any IT Assets, including content in Company-provided email accounts.

This is true regardless of the labeling of the IT Asset, data or communications, the use of encryption, the deletion of the data or communications, whether the situation involves personal use, or any other factor. The Company may also perform the recording and analysis for other lawful purposes, which vary by country. For example, in the United States, there is no legal limitation on the Company's right to engage in this monitoring, recording, and analysis, and You should have **no expectation of privacy** in anything described in this Systems Monitoring section. In fact, New York law requires that we provide the following statement to those of You in New York:

> "Any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio or electromagnetic, photoelectronic or photo-optical systems may be subject to monitoring at any and all times and by any lawful means."

For those reasons, our monitoring and recording may involve the collection and analysis of any kind of Your personal data and of others, such as:

- personal contents of emails, documents, and any other communications;

- information about devices issued by the Company (e.g., which devices were issued, number of devices, MAC address of device, phone number);

- device usage information (e.g., mobile data usage, battery usage, applications used, calls made, text messages sent);

- IP addresses;

- login and logout information;

- session length;

- log-in location;
- logs of applications used, downloads, uploads, and actions taken; and
- internet usage information (e.g., websites visited, applications downloaded).

4. Disclosures of Personal Data

We may share your personal data with the following parties:

- Company group entities and affiliates;
- service providers and vendors (e.g., suppliers and contractors who support the Company's operations including those who administer records, technological resource and cybersecurity support, recruitment, or training; professional advisers such as accountants, auditors and lawyers; consumer reporting agencies);
- government and law enforcement agencies; and
- potential acquirers or purchasers in relation to disposals of any of the Company's business or assets.

5. Your Data Rights

Subject to local law, you may have certain rights regarding personal data. For example, those of You who reside in California can use our Your Privacy Choices form, the Opt-Out Icon found on our website, or call (866) 958-9975 to ask to opt out of our "selling" or "sharing" of your personal data, in the very narrow way that the CCPA defines those terms and rights. (Under the CCPA, during the last 12 months, we "sold" and "shared" data about visitors to our public website as described in our website Privacy Policy, and that practice continues today, but we have not and do not "sell" or "share" personal information we collect in the context of an employment or other working relationship as the CCPA defines those terms.)

We do not engage in any use of "sensitive personal information" (within the meaning of the CCPA) for which the CCPA would require us to offer you the right to limit such use due to its sensitive nature.

Those of you who have other rights with respect to personal data can use our Your Privacy Choices form for the fastest response or email us at privacy@gaf.com. For example, residents of California can use those methods to exercise the rights described in the California section below, and Canadians can use those methods to exercise their rights to access their personal data; have inaccurate personal data corrected; request

that certain personal data be erased; or withdraw consent of our handling of personal data in certain cases.

To exercise any rights, you may be required to provide additional information to verify your identity or otherwise as necessary to assist the Company in fulfilling your request.

6. More Details for Those of You in California

This section applies only to those of You who reside in California. It does not cover personal information or practices that are exempt from the CCPA.

In 2024, we made the following disclosures of the following categories personal information that we collected that year:

Category of personal information collected about California residents in 2024	**Entities to whom we disclosed it**
Government-issued identifiers (e.g., Social Security number)	Affiliates, companies that assist us (such as benefits providers), governmental entities
Other identification and contact information and related identifiers	Affiliates, companies that assist us (such as benefits providers), governmental entities, customers
Professional or employment-related information	Affiliates, companies that assist us (such as benefits providers), governmental entities, customers
Education information	Affiliates, companies that assist us (such as background check providers),
Internet, electronic network, and device activity and device information and related identifiers, such as IP addresses and network traffic	Affiliates, companies that assist us (such as data storage and cybersecurity providers)

Communications	Affiliates, companies that assist us (such as data storage providers, email service providers, and cybersecurity providers), customers
Audio or visual information, such as voicemails and photos on our website	Affiliates, companies that assist us (such as web hosts, video conferencing providers, and the operator of our in-cab safety cameras)
Precise geolocation information (e.g., company trailer location)	Affiliates, companies that assist us, customers and other companies involved in our logistics operations
Health information	Affiliates, companies that assist us (such as benefits providers), governmental entities
Other legally protected classification information or characteristics of potentially protected classification information under California law (e.g., race or ethnicity)	Affiliates, companies that assist us (such as data storage providers), governmental entities

Subject to certain exceptions, you may request that we:

- provide access to and/or a copy of certain information we hold about you;
- correct inaccurate personal information about you;
- delete personal information you provided to us;
- provide you a description of categories of personal information we have collected or disclosed about you in the last twelve months;
- the categories of sources of such information;
- the business or commercial purpose for collecting or selling your personal information; and

- the categories of third parties with whom we shared personal information.

There are exceptions to certain rights listed above. For example, if an applicant in California requests deletion of their personal data, we still will need to maintain certain personal data.

Regardless, you have the right not to be discriminated against or retaliated against (as provided for in California law) for exercising your CCPA rights.

We have the right to take reasonable steps to verify your identity before responding to most types of CCPA requests. For example, in doing so, we may ask you for verification information so that we can match at least two verification points with information we maintain in our files about you, or we may ask you to verify your email address or login to an existing account you have with us. If we are unable to verify you through this method, we have the right, but not the obligation, to request additional information from you.

Californians have a right to designate an agent to exercise their CCPA rights on their behalf. The agent must use our online form (Your Privacy Choices) to make the request. We must receive a written authorization acceptable to us for the agent to act on your behalf. You may still need to verify your identity and confirm the agent's authority directly with us if we are not convinced of the validity of the agent's request. For security and legal reasons, we may refuse to accept requests that require us to visit an agent's website.

In addition, your browser may also offer a way to activate the Global Privacy Control signal ("GPC"). Our websites each treat qualifying browsers for which the user has activated the GPC signal as having opted out of what CCPA calls a "sale" or "sharing" of any California personal data that is collected on that site from that browser using cookies and similar technology. You can override that treatment for a GPC-enabled browser by using the cookie controls available from the website's footer.

We will keep most of your personal data until the position for which you applied has been filled, and for a reasonable period of time thereafter for EEO and other administrative tracking and reporting purposes. Once our relationship with you has come to an end, we will retain your personal data for a period of time that enables us to:

- maintain business records for analysis and/or audit purposes;
- comply with record retention requirements under applicable law;
- defend or raise any existing or potential legal claims; and
- respond to any queries or complaints you may have.

We plan to delete your personal data when we determine it is no longer required for these purposes. If you become an employee, your personal data will then be subject to

our Workforce Privacy Notice and our records retention program.

7. Contact Details

If you have any questions or wish to exercise any available rights, please contact us at privacy@gaf.com.

8. Changes to This Policy

The Company reserves the right to modify, revoke, suspend, terminate or change this policy, in whole or in part, at any time, with or without notice.

This policy does not and is not intended to create any employment relationship or contract or any guarantee of continued employment for any applicant or any other contractual or legal right.