



GREENBRIER COMPANIES, INC.'S PRIVACY NOTICE FOR CALIFORNIA RESIDENTS

Effective Date: January 1, 2023

Last Modified: April 17, 2024

This Privacy Notice for California Residents ("Notice") supplements the information contained in Greenbrier Companies, Inc.'s ("Greenbrier" or "we") Privacy Policy (<https://www.gbrx.com/legal/>) and applies solely to all visitors, users, employees, and others who reside in the State of California ("consumers" or "you"). We adopt this Notice to comply with the California Consumer Privacy Act of 2018 (the "CCPA") and the California Privacy Rights Act of 2020 (the "CPRA") (together with the CCPA, the "California Privacy Laws") and any terms defined in the California Privacy Laws have the same meaning when used in this Notice.

Information We Collect

We may collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular employee, consumer or device ("personal information"). Personal information does not include:

- Publicly available information from government records.
- Deidentified or aggregated consumer information.
- Information excluded from the California Privacy Laws' scope, like:
 - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the California Confidentiality of Medical Information Act ("CMIA"), clinical trial data, or other qualifying research data;
 - personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act ("FCRA"), the Gramm-Leach-Bliley Act ("GLBA") or California Financial Information Privacy Act ("FIPA"), and the Driver's Privacy Protection Act of 1994.

In particular, we may have collected the following categories of personal information from California residents within the last 12 months:

Category	Examples	Retention Period
A. Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol ("IP") address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers	As required by law or as long as necessary for a business purpose (such as employment), whichever is longer

<p>B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))</p>	<p>A name, signature, Social Security number, address, telephone number, passport number, driver's license or state identification card number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information</p> <p><i>*Some personal information included in this category may overlap with other categories.</i></p>	<p>As required by law or as long as necessary for a business purpose (such as employment), whichever is longer</p>
<p>C. Protected classification characteristics under California or federal law</p>	<p>Age (40 years or older), race, color, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status</p>	<p>As required by law or as long as necessary for a business purpose (such as employment), whichever is longer</p>
<p>D. Commercial information</p>	<p>Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies</p>	<p>As required by law or as long as necessary for a business purpose (such as for commercial marketing purposes), whichever is longer</p>
<p>E. Biometric information</p>	<p>Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data</p>	<p>Not Applicable (not collected)</p>
<p>F. Internet or other similar network activity</p>	<p>Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement</p>	<p>As required by law or as long as necessary for a business purpose (such as for commercial marketing</p>

		purposes), whichever is longer
G. Geolocation data	Physical location or movements	Not Applicable (not collected)
H. Sensory data	Audio, electronic, visual, thermal, olfactory, or similar information	Not Applicable (not collected)
I. Professional or employment-related information	Current or past job history or performance evaluations	As required by law or as long as necessary for a business purpose (such as for recruiting or employment), whichever is longer
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99))	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records	As required by law or as long as necessary for a business purpose (such as for recruiting or employment), whichever is longer
K. Inferences drawn from other personal information	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes	Not Applicable (not collected)

Sensitive Personal Information

Sensitive personal information (“SPI”) is a subtype of personal information consisting of specific information categories. In particular, we may have collected the below categories of SPI from California residents within the last 12 months. While we may collect information that falls within the SPI categories listed in the table below, California Privacy Laws do not treat this information as sensitive because we do not collect or use it to infer characteristics about a person.

SPI Category	Business Purpose(s)	Collection and/or Disclosure Details
Government identifiers , such as Social Security number, driver’s license, state identification card, or passport number	To recruit and process employment applications, including verifying eligibility for employment and conducting background and related checks	We never sell this information, and may only share it for the business purposes provided in this Notice. We only keep this information as required by law or as long as necessary for a business purpose, whichever is longer.

Racial or ethnic origin	<p>To conduct internal audits and investigate complaints, grievances, and suspected violations of our policies</p> <p>To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations</p>	<p>We never sell this information, and may only share it for the business purposes provided in this Notice. We only keep this information as required by law or as long as necessary for a business purpose, whichever is longer.</p>
Religious or philosophical beliefs	<p>To conduct internal audits and investigate complaints, grievances, and suspected violations of our policies</p> <p>To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations</p>	<p>We never sell this information, and may only share it for the business purposes provided in this Notice. We only keep this information as required by law or as long as necessary for a business purpose, whichever is longer.</p>
Union membership	<p>To conduct internal audits and investigate complaints, grievances, and suspected violations of our policies</p> <p>To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations</p>	<p>We never sell this information, and may only share it for the business purposes provided in this Notice. We only keep this information as required by law or as long as necessary for a business purpose, whichever is longer.</p>
Health information	<p>To conduct internal audits and investigate complaints, grievances, and suspected violations of our policies</p> <p>To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations</p>	<p>We never sell this information, and may only share it for the business purposes provided in this Notice. We only keep this information as required by law or as long as necessary for a business purpose, whichever is longer.</p>

Greenbrier may obtain the categories of personal information listed above from the following categories of sources:

- directly from a California resident (for example, from forms a California resident completes or products and services a California resident may purchase), or
- indirectly from a California resident (for example, from observing actions on our Website).

Use of Personal Information

In addition to the specific business purposes listed in the SPI chart, we may use or disclose a California resident's personal information we collect for one or more of the following purposes:

- to fulfill or meet the reason a California resident provided the information (For example, if a California resident shares their name and contact information to request a price quote or ask a question about our products or services, we may use that personal information to respond to such inquiry. If a California resident provides their personal information to purchase a product or service, we may use that information to process payment and facilitate delivery.
- to provide, support, personalize, and develop our Website, products, and services;
- to create, maintain, customize, and secure an account with us;
- to process requests, purchases, transactions, and payments and prevent transactional fraud;
- to provide support and to respond to inquiries, including to investigate and address concerns and monitor and improve our responses;
- to help maintain the safety, security, and integrity of our Website, products and services, databases and other technology assets, and business;
- for testing, research, analysis, and product development, including to develop and improve our Website, products, and services;
- to respond to law enforcement requests and as required by applicable law, court order, or governmental regulations;
- as described to you when collecting personal information of a California resident or as otherwise set forth in the California Privacy Laws;
- to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Greenbrier's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by Greenbrier about is among the assets transferred;
- to process an employment application;
- to assess an applicant's capabilities and qualifications for a job;
- to conduct reference checks;
- to respond to inquiries and communicate with applicants about their employment application, and to send you information regarding changes to our terms and policies;
- to comply with or monitor compliance with any applicable law or regulation;

- to conduct background checks if we offer a California resident a position of employment; and
- to preserve our other legitimate interests, for example, for Greenbrier’s administrative purposes, aggregate management reporting, internal training, and as generally required to conduct our business.

Greenbrier will not collect additional categories of personal information or use the personal information that we may have collected for materially different, unrelated, or incompatible purposes without providing appropriate notice.

Sharing Personal Information

Greenbrier may disclose personal information of a California resident to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.

We may share personal information of a California resident with the following categories of third parties:

- domain name service providers;
- hosting service providers;
- data analytics providers and Internet cookie data recipients, such as Google Analytics;
- government entities (if required);

Disclosures of Personal Information for a Business Purpose

In the preceding 12 months, Greenbrier may have disclosed the following categories of personal information from the chart above for a business purpose:

Category A: Identifiers

Category B: California Customer Records personal information categories

Category C: Protected classification characteristics under California or federal law

Category D: Commercial information

Category F: Internet or other similar network activity

Category I: Professional or employment-related information

Sales of Personal Information

In the preceding 12 months, Greenbrier HAS NOT SOLD personal information.

Your Rights and Choices

The California Privacy Laws provides consumers (California residents) with specific rights regarding their personal information. This section describes the California Privacy Laws rights available to California residents and explains how to exercise those rights.

Right to Know and Data Portability Rights

You have the right to request that Greenbrier disclose certain information to you about our collection and use of your personal information over the past 12 months (the “right to know”).

Once we receive your request and confirming your identity (see Exercising Access, Data Portability, and Deletion Rights), we will disclose to you:

- the categories of personal information that we may have collected about you;
- the categories of sources for the personal information that we may have collected about you;
- our business or commercial purpose for collecting or selling such personal information;
- the categories of third parties with whom we may have shared that personal information;
- the specific pieces of personal information we may have collected about you (also called a data portability request);
- if we sold or disclosed your personal information for a business purpose, two separate lists disclosing:
 - sales, identifying the personal information categories that each category of recipient purchased; and
 - disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

Right to Delete

You have the right to request that Greenbrier delete any of your personal information that we may have collected from you and retained, subject to certain exceptions (the “Right to Delete”). Once we receive and confirm your verifiable consumer request (see Exercising Your Rights to Know or Delete), we will review request to see if an exception allowing us to retain the information applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

1. complete the transaction for which we may have collected the personal information, provide a good or service that you may have requested, take actions reasonably anticipated within the context of any ongoing business relationship with you, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, or otherwise perform any contract with you;
2. detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
3. debug products to identify and repair errors that impair existing intended functionality;
4. exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law;
5. comply with the California Electronic Communications Privacy Act (Cal. Penal Code, § 1546 *et. seq.*);
6. engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information’s deletion may likely render impossible or seriously impair the research’s achievement, if you previously provided informed consent;
7. enable solely internal uses that are reasonably aligned with consumer expectations based on any relationship with us;
8. comply with a legal obligation; and/or

9. make other internal and lawful uses of that information that are compatible with the context in which you may have provided it.

Exercising Your Rights to Know or Delete

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

- calling us at 800-343-7188;
- emailing us at CCPA_Compliance@gbrx.com.

Only you, or someone legally authorized to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative; and
- describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot 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.

Making a verifiable consumer request does not require you to create an account with us.

We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We will confirm receipt of your request within 10 business days.

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to 45 days), we will inform you of the reason and extension period in writing.

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.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide any personal information we may have that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

We will only use personal information provided in an opt-out request to review and comply with the request.

Non-Discrimination

We will not discriminate against you for exercising any of your California Privacy Laws rights. Unless permitted by the California Privacy Laws, we will not:

- deny you goods or services;
- charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties;
- provide you a different level or quality of goods or services; or
- suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

However, we may offer you certain financial incentives permitted by the California Privacy Laws that *can result* in different prices, rates, or quality levels. Any California Privacy Laws-permitted financial incentive we offer will reasonably relate to your personal information's value and contain written terms that describe the program's material aspects. Participation in a financial incentive program requires your prior opt in consent, which you may revoke at any time.

Other California Privacy Rights

California's "Shine the Light" law (Civil Code Section 1798.83) permits users of our Website that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. However, please know that we DO NOT disclose information to third parties for their direct marketing purposes.

Changes to This Notice

Greenbrier reserves the right to amend this privacy notice at our discretion and at any time. When we make changes to this Notice, we will post the updated notice on the Website and update the notice's effective date. **Your continued use of our Website following the posting of changes constitutes your acceptance of such changes.**

Contact Information

If you have any questions or comments about this notice, the ways in which Greenbrier collects and uses any California resident's personal information described below and in the Privacy Policy, <https://www.gbrx.com/legal/>, your choices and rights regarding such use, or wish to exercise your rights under the California Privacy Laws, please do not hesitate to contact us at:

Phone: 800-343-7188

Website: www.gbrx.com

Email: CCPA_Compliance@gbrx.com