California Employee Privacy Policy

Effective Date: January 1, 2026

Last Updated on January 22, 2026

This California Employee Privacy Policy describes how Advance Beverage Company and its subsidiaries, affiliates, and related entities (collectively, "Advance," "Company," "we," or "us") collect and process personal information about our California employees. Under the California Consumer Privacy of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA), we are required to provide our 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, along with a description of the rights they have regarding their personal information. This Employee Privacy Policy provides the information the CCPA requires, together with other useful information regarding our collection and use of personal information, and any terms defined in the CCPA have the same meaning when used in this policy.

This Employee Privacy Policy applies to our prospective, current, and former employees who are California residents when the CCPA covers our collection and uses your personal information in the employment context.

This Employee Privacy Policy does not apply to our collection and use of personal information in a consumer or business-to-business capacity. For more information on our collection and use of consumer personal information, including how we process opt-out preference signals, please see our online privacy policy available at: https://advancebeverage.com/privacy-policy/.

Personal Information Collected

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

- Publicly available information, including from government records, through widely distributed media, or that the employee made publicly available without restricting it to a specific audience.
- Lawfully obtained, truthful information that is a matter of public concern.
- Deidentified or aggregated employee information.
- Information excluded from the CCPA's scope, like:
    - health or medical information covered by the Health Insurance Portability and Accountability Act (HIPAA) and the California Confidentiality of Medical Information Act (CMIA), clinical trial data, or other qualifying research data; or
    - personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act.

Personal Information Categories Chart

The chart below identifies which categories of personal information we collected from our employees within the last 12 months.

Category	Examples	Collected
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers, and similar information for your dependents and beneficiaries.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, photograph, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, membership in professional organizations, professional licenses and certifications, bank account number, credit card number, debit card number, or any other financial information,-medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	YES
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, national origin, citizenship, marital status, medical condition, physical or mental disability, sex including gender, gender identity, pregnancy or childbirth and related medical conditions, military and veteran status.	YES
D. Commercial information.	Records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	YES
E. Biometric information.	Facial Recognition, fingerprint, or hand punch/hand-geometry data collected by a biometric time clock	NO
F. Internet or other similar network activity.	All activity on our information systems (such as internet browsing history, search history, intranet activity, email communications, social media postings, stored documents and emails, usernames, and passwords) and all activity on the Company's communications systems (such as phone calls, call logs, voicemails, text messages, chat logs, app use, mobile browsing and search history, mobile email	YES

	communications, and other information about an employee's use of Company-issued devices.)	
G. Geolocation data.	Physical location or movements such as the time and physical location related to use of an internet website, application, or device, and GPS location data from mobile devices of employees who participate in our vehicle reimbursement program	YES
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information, including COVID-19 related temperature checks and call monitoring and video surveillance.	NO
I. Professional or employment-related information.	Current or past job history or performance evaluations, such as employment application information (work history, academic and professional qualifications, educational records, references, and interview notes, background check, drug testing results, work authorization, performance and disciplinary records, salary, bonus, commission, and other similar compensation data, benefit plan enrollment, participation, and claims information, leave of absence information including religious, military and family obligations, health data concerning employee and their family members).	YES
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.	NO
K. Inferences drawn from other personal information	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO
L. Sensitive personal information.	Further identified in the chart below.	YES

Sensitive Personal Information Categories Chart

Sensitive personal information is a subtype of personal information consisting of the specific information categories listed in the chart below. Importantly, the CCPA only treats this information as sensitive personal information when we collect or use it to infer characteristics about an employee.

The chart below identifies which sensitive personal information categories, if any, we have collected information from our employees to infer characteristics about them in the last 12 months.

Sensitive Personal Information Category	Collected to Infer Characteristics?
L.1. Government identifiers, such as your Social Security number (SSN), driver's license, state identification card, or passport number.	YES
L.2. Complete account access credentials, such as usernames, account logins, account numbers, or card numbers combined with required access/security code or password.	YES
L.3. Precise geolocation, such as physical access to a Company office location, or the location of a delivery, sales, or other employee in the field.	YES
L.4. Racial or ethnic origin.	YES
L.5. Citizenship or immigration status.	YES
L.6. Religious or philosophical beliefs.	NO
L.7. Union membership.	NO
L.8. Mail, email, or text messages not directed to the Company, but made on company devices	YES
L.9. Genetic data.	NO
L.10. Neural Data, such as information generated by measuring a consumer's central or peripheral nervous system's activity that is not inferred from nonneural information (effective January 1, 2025).	NO
L.11. Unique identifying biometric information.	NO
L.12. Health information, including job restrictions and workplace illness and injury information.	YES
L.13. Sex Life or Sexual Orientation Information	NO

Sources of Personal Information

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

- Directly from you, such as from the forms or information you input into the Company's ADP WORKFORCE NOW system.

- Indirectly from you, such as from your interactions with the Company's computer systems.
- From our service providers, such as temp agencies, ADP workforce now, Empower, Captrust, Anthem Blue Cross, DataQuest, ABC Occupational, Encompass, BrewU, and Gallagher Bassett.
- Government entities, such as for background check purposes.
- From other employees, such as from performance reviews or other observations and interactions.
- From inferences generated by the Company's computer systems.

How We Use Personal Information

Personal Information Collection, Use, and Disclosure Purposes

We may use and disclose personal information, including sensitive personal information, we collect to advance the Company's business purposes, specifically to:

- Comply with all applicable laws and regulations.
- Recruit and evaluate you as a job applicant and a candidate for employment.
- Conduct background checks and verify employment eligibility.
- Monitor and record your hours of work
- Manage your employment relationship with us, including for:
    - Determining your eligibility to work and fulfill our obligations to relevant government authorities
    - onboarding processes;
    - open and maintain your employee records;
    - maintain an internal employee directory and grant you access to internal systems;
    - communicate with you for internal business purposes or emergencies;
    - timekeeping, payroll, and expense report administration;
    - the design and administration of employee benefits plans and programs, including for leaves of absence;
    - employee training and development requirements;
    - monitoring your absence and sickness, make decisions relating to human resource allocation, salary and benefit changes and address other issues that may arise from absences
    - the creation, maintenance, and security of your online employee accounts;
    - arranging or reimbursing for travel, contacting you during travel, as necessary with travel service providers, or in an emergency situation

    - the provision of human resources management services and employee data maintenance and support services;
    - reaching you, your emergency contacts, and plan beneficiaries when needed, such as when you are not reachable or are injured or ill;
    - workers' compensation claims management;
    - improving employee productivity and the Company's efficiency, logistics, and supply chain management;
    - conflict of interest reporting;
    - fulfill our obligations to regulators (including demonstrating the suitability of employees for their role);
    - to allocate resources and process payments of benefits, salary, and other amounts owed to you
    - to reimburse you for use of your mobile phone or device for employment-related benefits
    - employee job performance, including goals and performance reviews, promotions, discipline, suitability for promotions and benefits, suitability for awards, job moves and staff restructuring, and termination;
    - ensuring compliance with Company information systems policies and procedures;
    - maintaining personnel records and comply with record retention requirements[; and]
    - other human resources purposes.
- Manage and monitor employee access to and prevent unauthorized access to or use of Company property, including its facilities, equipment, and systems.
- Design, implement, and promote the Company's diversity and inclusion programs
- Conduct internal audits and workplace investigations.
- Investigate and enforce compliance with and potential breaches of Company policies and procedures.
- Engage in corporate transactions requiring review of employee records, such as for evaluating potential Company mergers and acquisitions.
- Maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance.
- Perform workforce analytics, data analytics, and benchmarking.
- Administer and maintain the Company's operations, including for safety purposes.
- Exercise or defend the legal rights of the Company and its employees[,/ and] [affiliates,] customers[, contractors, and agents].
- Respond to law enforcement requests and as required by applicable law or court order.

- As described to you when collecting your personal information or as otherwise set forth in the CCPA.

Sensitive Personal Information Use and Disclosure Purposes

We may use or disclose sensitive personal information for the following statutorily approved reasons **(Permitted SPI Purposes)**:

- Performing actions that are necessary for our employment relationship and that an average employee in an employment relationship with us would reasonably expect, including for many of the purposes listed in the prior section, Personal Information Collection, Use, and Disclosure Purposes.
- Preventing, detecting, and investigating security incidents that compromise the availability, authenticity, integrity, and or confidentiality of stored or transmitted personal information.
- Defending against and prosecuting those responsible for malicious, deceptive, fraudulent, or illegal actions directed at the Company.
- Ensuring physical safety.
- Short-term, transient use, such as non-personalized advertising shown as part of an employee's current employment with us, if we do not:
    - disclose the sensitive personal information to another third party; or
    - use it to build a profile about the employee or otherwise alter the employee's experience outside their current employment with the Company.
- Services performed for the Company, including maintaining or servicing accounts, providing human resources and employee benefits administration, processing or fulfilling transactions, verifying employee information, processing payments, or providing financing, analytic services, storage, or similar services for the Company.
- Activities required to:
    - verify or maintain the quality or safety of a product, service, or device that we own, manufacture, had manufactured, or control; and
    - improve, upgrade, or enhance the service or device that we own, manufacture, had manufactured, or controlled.
- Collecting or processing sensitive personal information not for the purpose of inferring characteristics about an employee.

We do not use or disclose sensitive personal information for purposes other than the Permitted SPI Purposes/We may also use or disclose sensitive personal information for any of the purposes listed in the prior section, Personal Information Collection, Use, and Disclosure Purposes, subject to your limitation rights. For more on your right to limit the use of your sensitive personal information, see Your Rights and Choices.

Additional Categories or Other Purposes

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice and, if required by law, seeking your consent, before using your personal information for a new or unrelated purpose.

We may collect, process, and disclose aggregated or identified information about our employees for any purpose, without restriction.

Disclosing, Selling, or Sharing Personal Information

Business Purpose Disclosures

We may disclose the personal information we collect, including sensitive personal information, to others for the business purposes described in the Personal Information Collection, Use, and Disclosure Purposes section and the table below, such as to engage service providers to help us administer our human resources functions, payroll, benefits, or plans. For example, we may disclose information from the Company's equipment or your use of our network, systems, or equipment to a service provider that provides us with data and cybersecurity services.

We only make these business purpose disclosures under written contracts that describe the purposes, require the recipient to keep the personal information confidential, and prohibit using the disclosed information for any purpose except performing the contract.

The chart below identifies the categories of entities to whom we have disclosed our employees' personal information for a business purpose (see ***Category of Business Purpose Disclosure Recipients***) over the past 12 months, along with the personal information categories disclosed and the disclosure's business purposes.

Business Purposes Disclosure Recipient Category, Personal Information Category, and Purposes Chart

Category of Business Purpose Disclosure Recipients	Personal Information Categories Disclosed	Sensitive Personal Information Categories Disclosed	Business Purpose Disclosures
ADP WORKFORCE NOW	A. Identifiers. B. Personal information categories listed in the California Customer Records statue. C. Protected classification	L.1. Government identifiers. L.2. Complete account access credentials. L.3. Precise geolocation. L.4. Racial or ethnic origin. L.5. Citizenship or immigration status.	To process payroll and perform other human resources functions. To perform human resources management services and employee support services.

	characteristics under California or federal law. F. Internet or other similar network activity. G. Geolocation data. I. Professional or employment-related information.	L.8. Mail, email, or text messages contents not directed to the Company.	
ANTHEM BLUE CROSS	A. Identifiers. B. Personal information categories listed in the California Customer Records statue. C. Protected classification characteristics under California or federal law. F. Internet or other similar network activity. I. Professional or employment-related information.	L.1. Government identifiers. L.2. Complete account access credentials. L.8. Mail, email, or text messages contents not directed to the Company. L.12. Health information.	To provide and manage employee benefits.

EMPOWER	A. Identifiers. B. Personal information categories listed in the California Customer Records statue. C. Protected classification characteristics under California or federal law. F. Internet or other similar network activity. I. Professional or employment-related information.	L.1. Government identifiers. L.2. Complete account access credentials. L.8. Mail, email, or text messages contents not directed to the Company.	To provide and manage employee retirement.

Selling or Sharing Personal Information

In the employment context, we do not sell your personal information to third parties and have not sold it in the past 12 months. We do not share your personal information with third parties for cross-context behavioral advertising purposes and have not shared your personal information in the past 12 months.

Retention Period

We retain your information only for as long as is reasonably necessary and proportionate to accomplish the purposes described in this Privacy Notice. Retention periods are determined based on factors such as the duration of your employment or engagement with us and our legal and business obligations, including record-keeping requirements, dispute resolution, and enforcement of our agreements. In some cases, this may require retaining information beyond the conclusion of your job application process or engagement. All retention and destruction of information is conducted in accordance with applicable law. When your information is no longer needed or, in any event, after legal authority to retain it has expired, your information may be destroyed, in accordance with applicable law

Your Rights and Choices

If you are a California employee, you have the following rights under the CCPA regarding your personal information:

Right to Know and Data Portability

You have the right to request that we disclose certain information to you about our collection and use of your personal information (the "**right to know**"), including the specific pieces of personal

information we have collected about you (a "**data portability request**"). Our response will cover the 12-month period preceding the request, although we will honor requests to cover a longer period that do not extend past January 1, 2022, unless doing so would be impossible or involves disproportionate effort. You may make **two** right to know and data portability requests in any 12-month period. Once we receive your request and confirm your identity (see How to Exercise Your Rights), we will disclose to you:

- The categories of:
  - personal information we collected about you; and
  - sources from which we collected your personal information.
- The business or commercial purpose for collecting your personal information and, if applicable, selling or sharing your personal information.
- If applicable, the categories of persons, including third parties, to whom we disclosed your personal information, including separate disclosures identifying the categories of your personal information that we:
  - disclosed for a business purpose to each category of persons; and
  - sold or shared to each category of third parties.
- When specifically requested, a copy of your personal information subject to any permitted redactions.

Right to Delete

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions and limitations (the "right to delete").

Right to Correct

You have the right to request correction of personal information we maintain about you that you believe is inaccurate. We may require you to provide documentation, if needed, to support your claim that the information is inaccurate. Unless an exception applies, we will correct personal information that our review determines is inaccurate and direct our service providers to take similar action. For more information, see Exercising the Rights to Know, Delete, or Correct.

Right to Limit Sensitive Personal Information Processing to Permitted SPI Purposes

You have a right to limit our use or disclosure of your sensitive personal information to only the Permitted SPI Purposes if we use or disclose it for purposes other than the Permitted SPI Purposes.

Right to Non-Discrimination

You have the right not to be discriminated against or retaliated against for exercising any of your privacy rights under the CCPA.

How to Exercise Your Rights

Exercising the Rights to Know, Delete, or Correct

To exercise the right to know, data portability, delete, or correct described above, please submit a verifiable request to us by either:

- Calling us at 661-833-3783
- Emailing us at Tianna.onsurez@advancebeverage.com

Please describe your request with sufficient detail so we can properly understand, evaluate, and respond to it. You or your authorized agent may only submit a request to know or for data portability twice within a 12-month period.

Exercising the Right to Limit or Opt-Out

You can submit your request to limit or opt-out through:

- Emailing Tianna.onsurez@advancebeverage.com
- Contacting Human Resources at 661-833-3783

You can also submit your request to opt-out of personal information sales and sharing through an opt-out preference signal.

Notice of Right to Opt-out of Sale/Sharing

Responding to Your Requests to Know, Delete, or Correct

We will confirm receipt of your request within ten business days. If you do not receive confirmation within the ten-day timeframe, please contact Tianna.onsurez@advancebeverage.com or call 661-833-3783.

We endeavor to substantively respond to a verifiable request within 45 days of its receipt. If we require more time (up to another 45 days), we will inform you of the reason and extension period in writing. We will deliver our written response to your email address provided. Our substantive response will tell you whether or not we have complied with your request. If we cannot comply with your request in whole or in part, we will explain the reason, subject to any legal or regulatory restrictions. Applicable law may allow or require us to refuse to provide you with access to some or all of the personal information that we hold about you, or we may have destroyed, deleted, or made your personal information anonymous in compliance with our record retention policies and obligations.

Any disclosures we provide will cover information for the 12-month period preceding the request's receipt date. We will consider requests to provide a longer disclosure period that do not extend past January 1, 2022, unless providing the longer timeframe would be impossible or involves disproportionate effort.

For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance. Contact Tianna.onsurez@advancebeverage.com or call 661-833-3783.

We do not charge a fee to process or respond to your verifiable 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.

Response and Timing on Rights to Limit or Opt-Out

In response to your request to limit or opt-out, we will process your request, as soon as feasibly possible, but no later than 15 business days from the date we receive the request. You do not need to create an account with us to exercise your limitation and opt-out rights. We will only use personal information provided from your request to comply with the request.

We will also notify our service providers, contractors, and certain other downstream recipients of your request to limit or opt-out and instruct them to both:

- Comply with your request.
- Forward the request to their own downstream recipients, if applicable.

We may deny opt-out requests if we have a good-faith, reasonable, and documented belief that the request is fraudulent and clearly explain our denial decision to the requestor.

Once you make a request to limit or opt-out, we will wait at least 12 months before asking you to reauthorize the use or disclosure of your sensitive personal information for purposes other than the Permitted SPI Purposes or personal information sales or sharing. However, you may change your mind and opt back in at any time by:

Privacy Policy Changes

We reserve the right to update this Employee Privacy Policy at any time. If we make any material changes to this Employee Privacy Policy, we will update the policy's effective date and post the updated policy on ADP Workforce Now and Advance Beverage Company website. We encourage you to check ADP Workforce Now and the Advance Beverage Company website to review the current Employee Privacy Policy in effect.

Contact Information

If you have any questions or comments about this policy, the ways in which we collect and use your information described here, your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at:

Phone: 661-833-3783

Website: ADP WORKFORCE NOW EMPLOYEE PORTAL

Email: Tianna.onsurez@advancebeverage.com

Postal Address:

Advance Beverage Company

Attn: HR DEPARTMENT

5200 District Blvd. Bakersfield, CA 93313

If you need to access this Employee Privacy Policy in an alternative format due to having a disability, please contact Tianna.onsurez@advancebeverage.com or 661-833-3783.