CALIFORNIA EMPLOYEE PRIVACY POLICY

ADP, Inc. and its affiliates (collectively, "**ADP**," "**we**," or "**us**") value the trust of our personnel and endeavor to protect the privacy of their Personal Data. The purpose of this California Employee Privacy Policy (the "**Policy**") is to notify our California associates, contingent workers, directors, dependents, and other personnel ("**you**") of the processing of information that can reasonably be linked with you and that we collect, use, and disclose in the context of you current or former role as our personnel ("**Personal Data**").

The Policy also applies to the beneficiaries of your employment benefits, such as the individuals who are on your health plan and the beneficiaries of your retirement accounts, as well as your emergency contacts. It is your responsibility to inform any such individuals about this Policy and ensure that you have the right to provide their Personal Data to us.

Collection and Disclosure of Personal Data

The following details which categories of Personal Data we collect and process, as well as which categories of Personal Data we disclose to third parties for our operational business and employment purposes, including within the 12 months preceding the date this Policy was last updated.

I. Categories of Personal Data

Identifiers
Such as name, contact information, IP address that can reasonably be linked or associated with a particular California resident or household, email address, account name, online identifiers, photo badges, beneficiary designations, and government-issued identifiers (e.g., Social Security number, driver's license number, passport number).

Personal Data as defined in the California Customer Records Law
Such as name, contact information, signature, Social Security number, passport number, and medical, insurance, financial, education and employment information.

Protected Class Information
Such as characteristics of protected classifications under California or federal law, such as sex, age, gender, race, disability, medical conditions and information, citizenship, national origin, military/veteran status, gender identity and expression, primary language, political affiliation/activities, immigration status, marital status, and requests for leave.

Commercial Information
Such as transaction information and corporate credit card account information for expense reporting, and financial details, including bank account information for direct deposit.

Biometric Information
Such as fingerprints, voiceprints, and faceprints.

Internet or Network Activity Information
Such as access and usage information regarding websites, applications and systems, information about online communications, including browsing and search history, timestamp information, and access and activity logs.

Geolocation Data
Such as device geolocation, geofencing data, or GPS.

Audio/Video Data
Audio, electronic, visual, and similar information, such as call and video recordings created in connection with our business activities, including voicemail and security camera footage and information about the use of electronic devices and systems.

Education Information covered under the federal Family Educational Rights and Privacy Act
Such as disciplinary records and confirmation of graduation.

Employment Information
Professional or employment-related information, such as work history and prior employer, information from reference checks, background screening information, employment application, membership in professional organizations, personnel files, personal qualifications and training, eligibility for promotions and other career-related information, work preferences, business expenses, wage and payroll information, benefit information, information on leaves of absence or PTO, performance reviews, information on internal investigations or disciplinary actions.

Inferences
Drawn from any of the Personal Data listed above to create a profile about, for example, an individual's preferences, characteristics, aptitudes, and abilities.

Sensitive Personal Data
Including Special Categories of Data as defined in the Workplace Code:

- Photographic images for security and compliance purposes;
- Racial or ethnic data for diversity programs and affirmative action requirements;
- Criminal data (including data relating to criminal behavior, criminal records, or proceedings regarding criminal or unlawful behavior) for background screen programs and conducting due diligence;
- Physical or mental health data for accommodating disabilities, providing accessibility services, onsite healthcare, managing occupational health and safety requirements, or addressing emergency health needs;
- Biometric data for protecting ADP and Staff assets, managing access, security and fraud prevention;
- Religion or beliefs for tax withholdings or accommodating dietary restrictions; and

- Sexual preferences for providing benefits to Associates' spouses or domestic partners, or to facilitate diversity programs.

And

- Security, driver's license, state Identification card, or passport number.
- Account log-In, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
- A consumer's precise geolocation.
- Personal emails or text messages

II. Disclosure to Which Categories of Third Parties for Operational Business Purposes

(a) Other ADP Group Companies including ADP, LLC in the United States, ADP Private Limited in India, and any other ADP entity in the world (e.g., via the Associate Portal and other communication/collaborative tools; if a manager works in another country), who will only Process your Personal Data for the purposes set forth above, for the provision of IT and back office services for the company, in accordance with the requirements of the ADP Workplace Privacy Code;
(b) Third Party suppliers, including IT suppliers, financial and insurance services companies, law firms, auditors, investigators, credit reference agencies and criminal records bureaus (where permitted by law), and to those companies that provide benefits and services to you;
(c) Government and welfare bodies and authorities, law enforcement agencies and courts in all of the countries where we operate and when required or permitted by law;
(d) Clients, suppliers and other business partners, when the provision of professional contact details and other Personal Data is necessary in the framework of the business relationship;
(e) With your consent, as directed by you (e.g., as reference to a potential new employer) or as needed to protect your vital interests, such as in the event of an emergency or natural disaster.

We may also disclose the above categories of Personal Data to a third party in the context of any reorganization, financing transaction, merger, sale, joint venture, partnership, assignment, transfer, or other disposition of all or any portion of our business, assets, or stock (including in connection with any bankruptcy or similar proceedings).

Sale of Personal Data

We do not "sell" or "share" your Personal Data, including your Sensitive Personal Data, as defined under the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act. We have not engaged in such activities in the 12 months preceding the date this Policy was last updated. Without limiting the foregoing, we do not "sell" or "share" the Personal Data, including the Sensitive Personal Data, of minors under 16 years of age.

Sources of Personal Data

We collect, Process, and transfer the Personal Data which you provide to us as well as information obtained from other sources, including but not limited to recruiters, your previous employers or references, websites, credit reference agencies, government bodies and Third Parties who provide employment

background screening services or who assist us with internal investigation, only if permitted by law. The collecting, Processing, and transferring of your Personal Data is aligned with the commitments made in the ADP Workplace Privacy Code.

Purposes for the Collection and Use of Personal Data

ADP Processes Personal Data (including Sensitive Personal Data) pertaining to associates, contingent workers, directors, dependents, and other personnel as needed to provide as required by EEA Applicable Law and for approved Business Purposes, including:

(a) Payroll, human resources and personnel management;
(b) Contract personnel management;
(c) Business process execution and internal management;
(d) Health, safety, security and integrity;
(e) Organizational analysis and development, management reporting and acquisition and divestitures;
(f) Compliance with law; and
(g) Protecting the vital interests of Individuals.

Personal Data may be Processed for a Secondary Purpose, similar to the legitimate Business Purpose, provided appropriate additional measures are taken, including:

(a) Disaster recovery and business continuity, including transferring the information to an Archive;
(b) Internal audits or investigations;
(c) Implementation or verification of business controls;
(d) Statistical, historical, or scientific research;
(e) Dispute resolution;
(f) Legal or business counseling;
(g) Compliance with laws and company policies; or
(h) Insurance purposes.

Personal Data Retention Period

ADP will only retain your information for as long as necessary for the Purposes for which the Personal Data is processed. ADP has implemented a Global Records Information Management (RIM) Policy and has established records retention schedules for all types of Personal Data that ADP processes. Personal Data is retained in accordance with the records retention schedules to ensure that records containing Personal Data are retained as needed to fulfill the applicable Business Purposes, to comply with applicable laws, or as advisable in light of applicable statutes of limitations. When the retention period has expired, records containing Personal Data will be securely deleted or destroyed, de-identified, or transferred to archive, in accordance with the applicable records retention schedule.

Individual Right Requests specific to California Residents

You may, subject to applicable law, make the following requests:

(1) ***Right to Know*** - You may request that we disclose to you the following information covering the 12 months preceding your request:
   a. The categories of Personal Data we collected about you and the categories of sources from which we collected such Personal Data;
   b. The business or commercial purpose for collecting Personal Data about you; and
   c. The categories of Personal Data about you that we otherwise disclosed, and the categories of third parties to whom we disclosed such Personal Data (if applicable).

   A right to access will also include specific pieces of Personal data we collected about you. Personal Data that includes social security number, driver's license or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security question and answers, or unique biometric data generated from measurements or technical analysis of human characteristics, if applicable, will not be provided to protect the security this type of data.

   A copy of the Personal Data will be provided by us in a portable format.

(2) ***Right to Correction*** - You may request that we correct inaccuracies in your Personal Data.
(3) ***Right to Request Deletion of your Personal Data*** - You may request that we to have your Personal Data deleted.
(4) ***Right to Non-Discrimination*** - We will not discriminate against you if you choose to exercise your right under the California Privacy Rights Act (i.e., deny or provide you different level or quality of service).

How to Submit a California Rights Request

We will not unlawfully retaliate against you for making an individual request. To make a request, please send an email to myHRSupport@adp.com mailto:myHRSupport@adp.comor contact GHRSS at 1-877-237-4711. We will verify and respond to your request consistent with applicable law, taking into account the type and sensitivity of the Personal Data subject to the request. We may need to request additional Personal Data from you, such as associate ID, zip code of home address, month, and date of birth, in order to verify your identity and protect against fraudulent requests. If you maintain a password-protected account with us, we may verify your identity through our existing authentication practices for your account and require you to re-authenticate yourself before disclosing or deleting your Personal Data. If you make a request to delete, we may ask you to confirm your request before we delete your Personal Data.

Authorized Agents Submitting a Rights Request on Your Behalf

If an agent would like to make a request on your behalf as permitted by applicable law, the agent may use the submission methods noted in the section entitled "Individual Requests." As part of our verification process, we may request that the agent provide, as applicable, proof concerning their status as an authorized agent. In addition, we may require that you verify your identity as described in the section entitled "Individual Requests" or confirm that you provided the agent permission to submit the request.

Changes to this California Employee Privacy Policy

We may change or update this Policy from time to time. When we do, we will communicate changes and updates to this Policy by posting the updated Policy on this page with a new "Last Updated" date.

Contact Us

If you have any questions regarding this Policy, please visit the ADP Associate Portal, refer to the ADP Workplace Code, contact your local Human Resources manager, or send an email to myHRsupport@adp.com.