

EFFECTIVE DATE: January 1, 2020

LAST UPDATED: February 23, 2023

CALIFORNIA CONSUMER PRIVACY STATEMENT

Pursuant to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (collectively, the “CCPA”), ADP, Inc. and its affiliates (“ADP,” “we,” or “us”) are providing the following Privacy Statement to explain how ADP collects, uses and discloses Personal Data that we collect from individuals who are residents of California, including but not limited to users who visit our websites or consumers who receive services directly from ADP. This Privacy Statement does not apply to Personal Data pertaining to ADP employees or employees of ADP clients where ADP is acting in its capacity as a service provider.

For purposes of this Privacy Statement, Personal Data is information that identifies, relates to, or could reasonably be linked with a particular California resident or household.

ADP also has a Global Data Privacy Policy that applies to all ADP companies worldwide. An overview of our Privacy Program is located at www.adp.com/dataprivacy.

Collection, Disclosure, and Sharing of Personal Data

The following details which categories of Personal Data we collect and process, which categories of third parties may have access to your Personal Data for operational business purposes, as well as which categories of Personal Data we “share” for purposes of cross-context behavioral advertising, including within the 12 months preceding the date this Privacy Statement was last updated.

Categories of Personal Information	Disclosed to Which Categories of Third Parties for Operational Business Purposes <i>(see below for a more detailed description of these categories)</i>	Shared with Which Categories of Third Parties for Cross-Context Behavioral Advertising
Identifiers , such as name, contact information, unique personal identifiers, email address, IP address, online identifiers, government-issued identifiers.	Service Providers/Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	Ad networks.
Personal information as defined in the California customer records law , such as name, contact information, financial, education, employment information.	Service Providers/Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	None.

Categories of Personal Information	Disclosed to Which Categories of Third Parties for Operational Business Purposes <i>(see below for a more detailed description of these categories)</i>	Shared with Which Categories of Third Parties for Cross-Context Behavioral Advertising
Characteristics of protected classifications under California or federal law , such as race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, sex, gender expression, gender identify, age, sexual orientation, military or veteran status.	Service Providers/Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	None.
Commercial Information , such as transaction information and purchase history, including purchases considered, consuming histories or tendencies.	Service Providers/Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	None.
Biometric Information , such as fingerprints, voiceprints and faceprints.	Not Applicable.	Not Applicable.
Internet or network activity information , such as IP address, mobile device ids, MAC address, browsing history, search history.	Service Providers/Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	Ad networks.
Geolocation Data , such as precise location/tracking data and coarse location/tracking data.	Service Providers/Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	None.
Audio/Video Data , such as photographs.	Service Providers/Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a	None.

Categories of Personal Information	Disclosed to Which Categories of Third Parties for Operational Business Purposes <i>(see below for a more detailed description of these categories)</i>	Shared with Which Categories of Third Parties for Cross-Context Behavioral Advertising
	Corporate Transaction, with your consent.	
Education Information subject to the federal Family Educational Rights and Privacy Act such as education and training history, education degrees, qualifications/certifications.	Service Providers/Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	None.
Employment Information. Professional or employment-related information, such as professional or employment related information such as work history and prior employer, background checks, performance rating or feedback, employer, occupation title/job role.	Service Providers/Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	None.
Inferences such as any assumptions drawn from any of the Personal Data listed above to create a profile about, for example, an individual’s preferences or characteristics. This is only applicable to consumers that purchase our TMBC product due to the nature of the product.	Service Providers/Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	None.
Sensitive Personal Information , such as social 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; precise geolocation; racial or ethnic origin, religious or philosophical beliefs, citizenship, immigration status, union membership.	Service Providers/Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	None.

Detailed Description of Categories of Third Parties

Third Parties that ADP may disclose your Personal Data are as follows:

(a) Service Providers/Subcontractors

ADP may share your Personal Data with our subcontractors for certain business purposes. This information is provided in order for them to provide ADP with services such as payment processing, advertising services, marketing partners, web analytics, data processing, IT services, customer support and other services such as for the purpose of auditing and fraud investigations.

(b) Related Entities

ADP may share Personal Data between and among ADP, its subsidiaries, and affiliated companies for purposes of management and analysis, and other business purposes. For instances, ADP may share your Personal Data with our subsidiaries and affiliated companies to expand and promote our product and service offerings.

(c) Law Enforcement/Legal Authorities

ADP may be required to disclose your Personal Data to third parties including law enforcement agencies when required to protect and defend our legal rights, protect the safety and security of users of our Services, prevent fraud, respond to legal process, or a request for cooperation by a government entity, as required by law.

(d) Corporate Transactions

In the event of sale, transfer, merger, reorganization, or similar event, ADP may transfer your Personal Data to one or more third parties as part of that transaction with the business entities or people involved in the deal negotiation or transfer.

(e) With Your Consent

ADP may share Personal Data about you with other third-party companies if you give us permission or direct us to share the information. ADP will share Personal Data with authorized agents that you authorize ADP to communicate to.

We do not sell and have not sold Personal Data, including your Sensitive Personal Data, in the preceding 12 months. Without limiting the foregoing, we do not sell the Personal Data, including the Sensitive Personal Data, of minors under 16 years of age. We do not knowingly “share” the Personal Data, including the Sensitive Personal Data, of minors under 16 years of age.

Sources of Personal Data

We collect this Personal Data actively (e.g. direct input from individual) or passively (e.g. website cookies) from you. Additionally, we may also collect Personal Data from third-party sources, such as our affiliates, business partners, and service providers.

Purposes for the Collection, Use and Sharing of Personal Data

ADP uses your Personal Data for the following Business Purposes and objectives:

- (a) Business Purposes for processing Personal Data pertaining to consumers. Personal Data pertaining to consumers with whom ADP has a business relationship may be processed as needed:**

- (1) To provide the information, product, or service requested by the individual, and as would be reasonably expected by the individual given the context in which the Personal Data was collected, and the information provided in the applicable privacy statement given to the individual (such as for personalization, remembering preferences, or respecting individual rights);
 - (2) For due diligence, including verifying the identity of the individual, as well as the eligibility of the individual to receive information, products, or services (such as verifying age, employment, or account status);
 - (3) To send transactional communications (such as requests for information, responses to requests for information, orders, confirmations, training materials, and service updates);
 - (4) To manage the individual's account, such as for customer service, finance, and dispute resolution purposes;
 - (5) For risk management and mitigation, including for audit and insurance functions, and as needed to license and protect intellectual property and other assets;
 - (6) For security management, including monitoring individuals with access to the website; applications, systems, or facilities, investigation of threats, and as needed for any data security breach notification; and
 - (7) To anonymize or de-identify the Personal Data. Where we maintain or use de-identified information, we will continue to maintain and use such information only in a de-identified fashion and will not attempt to re-identify such information.
- (b) Business-necessary processing activities.** ADP may process Personal Data as needed (i) to protect the privacy and security of the Personal Data it maintains, such as in connection with advanced security initiatives and threat detection; (ii) for treasury operations and money movement activities; (iii) for compliance functions, including screening individuals against sanction lists in connection with anti-money laundering programs; (iv) for business structuring activities, including mergers, acquisitions, and divestitures; and (v) for business activities, management reporting, and analysis.
- (c) Development and improvement of products and/or services.** ADP may process Personal Data to develop and improve its products and/or services, and for research, development, analytics, and business intelligence.
- (d) Relationship management and marketing.** ADP may process Personal Data for relationship management and marketing. This purpose includes sending marketing and promotional communications to individuals who have not objected to receiving such messages, such as product and service marketing communications, investor communications, Client communications (e.g., HR compliance alerts, product updates, and training opportunities and invitations to ADP events), customer satisfaction surveys, supplier communications (e.g., requests for proposals), corporate communications, and ADP news.
- (e) Operational purposes.** Additionally, ADP uses your Personal Data for purposes such as: (i) disaster recovery and business continuity; (ii) internal audits or investigations; (iii) implementation or verification of business controls; (iv) statistical, historical, or scientific research; (v) dispute resolution; (vi) legal or business counseling; (vii) compliance with laws and company policies; and/or (viii) insurance purposes.

Purposes for the Collection and Use of Sensitive Personal Data

Subject to your consent where required by applicable law, we may use Sensitive Personal Data for purposes of performing services for our business, providing goods or services as requested by you, ensuring security and integrity, short term transient use such as displaying first party, non-personalized advertising, servicing accounts, providing customer service, verifying customer information, processing payments, and activities relating to quality or product improvement.

Retention Period

We retain Personal Data for as long as needed or permitted in light of the purpose(s) for which it was collected. The criteria used to determine our retention periods include:

- (a) The length of time we have an ongoing relationship with you and provide services to you (for example, for as long as you have an account with us or keep using our services) and the length of time thereafter during which we may have a legitimate need to reference your Personal Data to address issues that may arise;
- (b) Whether there is a legal obligation to which we are subject (for example, certain laws require us to keep records of your transactions for a certain period of time before we can delete them); or
- (c) Whether retention is advisable in light of our legal position (such as in regard to applicable statutes of limitations, litigation or regulatory investigations).

California Consumer Rights

If you are a California resident you may make the following requests, subject to applicable law:

- (a) **Right to Access and Know** -- You may request that we disclose to you the following information:
 - (1) The categories of Personal Data we collected about you and the categories of sources from which we collected such Personal Data;
 - (2) The specific pieces of Personal Data we collected about you;
 - (3) The business or commercial purpose for collecting or sharing Personal Data about you;
 - (4) The categories of Personal Data about you that we shared (as defined under the applicable privacy law) and the categories of third parties with whom we shared such Personal Data; and
 - (5) 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).
- (b) **Right to Request Correction of your Personal Data** -- You may request to correct inaccuracies in your Personal Data;
- (c) **Right to Request Deletion of your Personal Data** -- You may request to have your Personal Data deleted; and
- (d) **Right to Opt-out of Sharing for Cross-Context Behavioral Advertising** -- You may request to opt out of the "sharing" of your Personal Data for purposes of cross-context behavioral advertising.

We will not unlawfully discriminate against you for exercising your rights under the CCPA.

How to Submit a California Rights Request

To make a privacy request, please contact us by clicking [here](#) or by emailing us at privacy@adp.com. 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 your name and email address, 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.

To request to opt out of any future sharing of your Personal Data for purposes of cross-context behavioral advertising, please go to www.adp.com and click the Cookie Preferences – Do Not Share My Data link at the bottom of the page to toggle off advertising cookies.

Authorized Agents Submitting a Request on Behalf of a Consumer

You may choose to designate an authorized agent to make a request under the CCPA on your behalf. No information will be disclosed until the authorized agent's authority has been reviewed and verified. Agents may be asked to provide proof of their status as an authorized agent. Once a request has been submitted by an authorized agent, we may require additional information from you to verify your identity as described in the section entitled "How to Submit a California Rights Request" or confirm that you provided the agent permission to submit the request. Authorized agents click [here](#) to submit a request.

Changes to this California Consumer Privacy Statement

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

Contact Us

If you have any questions regarding this California Consumer Privacy Statement, please contact us at privacy@adp.com. You may also reach us at:

ADP
ADP Global Data Privacy and Governance Team
MS 325
One ADP Boulevard
Roseland, NJ 07068-1728 USA