

ADP BrightJump Consumer Privacy Statement

Effective Date: June 18, 2020

Last Updated: October 31, 2024

This Consumer Privacy Statement explains how Automatic Data Processing Inc., all its consolidated subsidiaries, and ADP BrightJump (an ADP offering) (hereinafter "ADP", "ADP name of service", "our", or "we"), uses and discloses Personal Data that is collected through ADP BrightJump, which includes all webpages associated with ADP BrightJump, all application programming interfaces (APIs), file transfers and csv uploads, and all applications and communication tools provided by ADP BrightJump when you interact with ADP as a consumer or website user.

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.

This Privacy Statement explains how ADP uses and discloses Personal Data that we collect from individuals who engage with us as direct consumers of our products or services. Personal Data is any information that identifies you as an individual or relates to an identifiable individual.

1. Types of Personal Data

This Privacy Statement explains our practices regarding Personal Data collected by ADP BrightJump for the purposes of this offering, product, or service.

Some examples of Personal Data collected when you use ADP BrightJump include your name, address, email address, user profile information, employment information, demographic data, and any other information included on your resume when you choose to share your resume with us, social media profile (e.g. LinkedIn), or other information about how you engage with the offering.

2. How ADP BrightJump Collects Personal Data & Categories of Personal Data Collected

In most cases, we will collect Personal Data directly from you as a data controller. With your permission, we will obtain Personal Data directly from you including: your name, email address, mailing address, phone number, geographic location (city or area), education, employment history, skills and qualifications, any other information included on your resume when you choose to share your resume with us, and your IP address.

If you created a BrightJump account in connection with the submission of a job application on an ADP site, ADP BrightJump will also import Personal Data, including your name, email address, and resume

from that system of record. We may also collect the name of the company and role that you submitted an application for.

We will also ask you for Personal Data when you interact with us, such as when you register on ADP BrightJump, set up an account, sign up to receive marketing communications, or request our services.

We need to collect Personal Data to provide the requested services to you. If you do not provide the information requested, we may not be able to provide the services. If you disclose any Personal Data relating to other people to us or to our service providers in connection with ADP BrightJump, you represent that you have the authority to do so and to permit us to use the Personal Data in accordance with this Privacy Statement.

If you interact with us through our website, we use cookies and other online tracking technologies to collect information about your device and your use of ADP BrightJump.

For more information about cookies and other online tracking technologies, please see the section **“Cookies and Other Automatic Data Collection Technologies”** below.

3. How ADP BrightJump uses Personal Data

ADP BrightJump is an offering on ADP web properties that offers consumers tools to find job opportunities, prepare and submit job applications, access career coaches, and learn career skills. If a consumer elects to make their profile visible to recruiters, consumers may also be contacted about relevant job opportunities. ADP BrightJump uses Personal Data to customize the products and services offered to consumers. ADP BrightJump also uses Personal Data to facilitate the creation of consumer accounts with the third party offering the product or service, and account management support, and customer service.

We also use your Personal Data for the following business purposes:

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

We engage in these activities to manage our contractual relationship with you, to comply with a legal obligation, and/or based on our legitimate interest.

- (b) Business-necessary processing activities.** We 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 business structuring activities, including mergers, acquisitions, and divestitures; and (iii) for business activities, management reporting, and analysis.

We engage in these activities to manage our contractual relationship with you, to comply with a legal obligation, and/or based on our legitimate interest.

- (c) Development and improvement of products and/or services.** We process Personal Data to develop and improve its products and/or services, and for research, development, analytics, and business intelligence.

We engage in these activities based on our legitimate interest.

- (d) Relationship management and marketing.** We process Personal Data for relationship management, marketing, and to provide personalized services. 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, customer satisfaction surveys, and ADP news.

We will engage in these activities based on our legitimate interests, and with your consent to the extent required by applicable law.

- (e) Operational purposes.** Additionally, we use 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.

We engage in these activities to manage our contractual relationship with you, to comply with a legal obligation, and/or based on our legitimate interest.

4. Why and How Personal Data is disclosed by ADP BrightJump

ADP BrightJump does not provide your Personal Data to third parties for their own marketing purposes.

We limit our sharing of your Personal Data to:

- When you elect to make your profile visible to recruiters, we may share your name and any information in your profile with ADP clients so that they can contact you about job opportunities.
- ADP Group Companies, which use your Personal Data for the purposes listed in this Privacy Statement;
- Our service providers, to facilitate services they provide to us. These can include providers of such services as website hosting, data analysis, payment processing, order fulfillment, fraud

prevention, information technology and related infrastructure provision, customer service, email delivery, and auditing;

- Uses necessary to enforce our rights, protect our property, protect the rights, property or safety of others, in connection with any proposed or actual reorganization, bankruptcy, merger, sale, joint venture, assignment, transfer of ADP, or other disposition of all or any portion of ADP business or assets, or as needed to support external auditing, compliance and corporate governance functions;
- Third parties, including law enforcement agencies when required and to protect and defend our legal rights, protect the safety and security of users of our services, prevent fraud, respond to legal process (e.g. subpoena or court order), or a request for cooperation by a government entity, including as required by law.

5. Additional US State Specific Privacy Disclosure

The following table details the categories of Personal Data we collect and process, which categories of third parties may have access to your Personal Data for operational or business purposes, as well as which categories of Personal Data we “share” for purposes of cross-context behavioral or targeted 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>	Processing Purposes <i>(See section 3 How ADP uses your data for complete list)</i>	Shared with Which Categories of Third Parties for Cross-Context Behavioral or Targeted 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.	a (1, 2, 3, 4, 6, 7), b, d	Ad networks. <i>(See Opt-Out sharing of Personal Data section below for your options.)</i>
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.	a (1, 2, 3, 4, 6, 7), b, d	Ad networks. <i>(See Opt-Out sharing of Personal Data section below for your options.)</i>
Characteristics of protected classifications under California or federal law , such as race, religious creed, color, national origin,	Not applicable.	Not applicable	Not Applicable.

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>	Processing Purposes <i>(See section 3 How ADP uses your data for complete list)</i>	Shared with Which Categories of Third Parties for Cross-Context Behavioral or Targeted Advertising
ancestry, physical disability, mental disability, medical condition, marital status, sex, gender expression, gender identify, age, sexual orientation, military or veteran status.			
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.	a (1, 2, 3, 4, 6, 7), b, c, d	None.
Biometric Information , such as fingerprints, voiceprints and faceprints.	Not Applicable.	Not applicable	Not Applicable.
Internet or network activity information , such as IP address, mobile device ids, MAC address, browsing history, search history.	Not applicable.	Not applicable	Not applicable
Geolocation Data , such as precise location/tracking data and coarse location/tracking data.	Not applicable.	Not applicable	Not applicable
Audio/Video Data , such as photographs.	Service Providers / Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	a1, c	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>	Processing Purposes <i>(See section 3 How ADP uses your data for complete list)</i>	Shared with Which Categories of Third Parties for Cross-Context Behavioral or Targeted Advertising
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.	a (1, 2, 3, 4, 6, 7), b, c, d	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.	a (1, 2, 3, 4, 6, 7), b, c, d	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.	Service Providers / Subcontractors, Related Entities, Law enforcement/Legal authorities, Third Parties in the event of a Corporate Transaction, with your consent.	a (1, 2, 3, 4, 6, 7), b, c, d	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	Not applicable.	Not applicable	Not applicable

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>	Processing Purposes <i>(See section 3 How ADP uses your data for complete list)</i>	Shared with Which Categories of Third Parties for Cross-Context Behavioral or Targeted Advertising
origin, religious or philosophical beliefs, citizenship, immigration status, union membership; mental or physical health diagnoses, condition, history or treatment, sexual orientation and sex life; Personal Data collected from a known child.			

Opt-out of Sharing of Personal Data

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

Detailed Description of Categories of Third Parties

Third Parties to which we may disclose your Personal Data are as follows:

(a) Service Providers/Subcontractors

We may share your Personal Data with our service providers/subcontractors for certain business purposes. This information is provided in order for them to provide us 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

We may share Personal Data between and among ADP, its subsidiaries, and affiliated companies for purposes of management and analysis, and other business purposes. For instance, we 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

We may be required to disclose your Personal Data to third parties including law enforcement agencies when required and to protect and defend our legal rights, protect the safety and security of users of our services, prevent fraud, respond to legal process (e.g. subpoena or court order), or a request for cooperation by a government entity, including as required by law.

(d) Corporate Transactions

In the event of sale, transfer, merger, reorganization, or similar event, we 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

We may share Personal Data about you with other third-party companies if you give us permission or direct us to share the information. We will share Personal Data with authorized agents that you authorize ADP to communicate to, including sharing your name and profile with ADP clients if you elect to make your profile visible to recruiters.

We do not sell and have not sold Personal Data, including your Sensitive Personal Data, in the preceding 12 months.

Sources of Personal Data

We collect this Personal Data actively (e.g. direct input from individuals) 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.

6. Cookies and Other Automatic Data Collection Technologies

When you visit our website or use our mobile applications, we collect certain information by automated means, using technologies such as cookies, pixel tags, browser analysis tools, server logs, and web beacons. For example, when you visit our website, we place cookies on your computer. Cookies are small text files that websites send to your computer or other Internet-connected device to uniquely identify your browser or to store information or settings in your browser. Cookies allow us to recognize you when you return. They also help us provide a customized experience and enable us to detect certain kinds of fraud. In many cases, you can manage cookie preferences and opt-out of having cookies and other data collection technologies used by adjusting the settings on your browser. All browsers are different, so visit the “help” section of your browser to learn about cookie preferences and other privacy settings that may be available.

Pixel tags and web beacons are tiny graphic images placed on website pages or in our emails that allow us to determine whether you have performed a specific action. When you access these pages or open or click an email, the pixel tags and web beacons generate a notice of that action. These tools allow us to measure response to our communications and improve our web pages and promotions.

We collect many different types of information from cookies and other technologies. For example, we collect information from the device you use to access our website, your operating system type, browser type, domain, and other system settings, as well as the language your system uses and the country and time zone where your device is located. Our server logs also record the Internet Protocol (IP) address assigned to the device you use to connect to the Internet. An IP address is a unique number that devices use to identify and communicate with each other on the Internet. We may also collect information about the website you were visiting before you came to ADP and the website you visit after you leave our site.

In many cases, the information we collect using cookies and other tools is only used in a non-identifiable way, without reference to Personal Data. For example, we use information we collect about website users to optimize our websites and to understand website traffic patterns. In some cases, we do

associate the information we collect using cookies and other technology with your Personal Data. This Privacy Statement applies to the information when we associate it with your Personal Data.

Our website may include embedded YouTube videos. When you click on an embedded YouTube video that video is loaded from a domain operated by YouTube. Although we have enabled the Privacy-Enhanced mode for embedded YouTube videos, which prevents YouTube from placing tracking cookies on your device when viewing these videos on our site, YouTube may collect your IP address and other devices information for their own purposes. To learn more about YouTube's Privacy-Enhanced mode visit the YouTube support page at <https://support.google.com/youtube/answer/171780?hl=en-GB&ref=axbom.com#>. To learn more about YouTube's processing of IP addresses visit YouTube's privacy policy at <https://policies.google.com/privacy?sjid=60584270626491410-NA>.

We use third-party advertising companies to serve advertisements regarding goods and services that may be of interest to you when you access and use ADP BrightJump and other websites or online services. You may receive advertisements based on information relating to your access to and use of ADP BrightJump and other websites or online services on any of your devices, as well as on information received from third parties. These companies place or recognize a unique cookie on your browser (including through the use of pixel tags). They also use these technologies, along with information they collect about your online use, to recognize you across the devices you use, such as a mobile phone and a laptop.

If you would like more information about this practice, and to learn how to opt out of it in desktop and mobile browsers on the particular device on which you are accessing this Privacy Statement, please visit <http://optout.aboutads.info/#/> and <http://optout.networkadvertising.org/#/>. You may download the AppChoices app at www.aboutads.info/appchoices to opt out in mobile apps.

Although our website currently does not have a mechanism to recognize the various web browser Do Not Track signals, we do offer consumers choices to manage their preferences that are provided in the previous sections above. To learn more about browser tracking signals and Do Not Track please visit <http://www.allaboutdnt.org/>.

We also process opt-out preference signals, such as the Global Privacy Control (GPC). The GPC is a mechanism that enables consumers to automatically communicate their privacy preferences to opt-out of sale and sharing of their personal information to this website. This ensures that the consumer's opt-out preference is honored through compatible browsers or extensions that support GPC, consistently across all websites accessed through the browser or device you are using. Go to your browser's setting to enable GPC. If enabled you will receive notification or see a visual indication (e.g., banner or pop-up message) on our site confirming that your GPC signal has been detected and your opt-out request has been processed. For information about how to use the Global Privacy Control, please visit <https://globalprivacycontrol.org/>.

7. Third-Party Analytics

ADP BrightJump uses third-party analytics providers, such as Google Analytics. This service uses cookies and similar technologies to collect and analyze information about the use of ADP BrightJump and report on activities and trends. These services may also collect information regarding the use of other websites, apps and online resources. You can learn about Google's practices by going to www.google.com/policies/privacy/partners/ and exercise the opt-out provided by Google by

downloading the Google Analytics opt-out browser add-on, available at <https://tools.google.com/dlpage/gaoptout>.

8. Invisible reCAPTCHA

We use Google's invisible reCAPTCHA application in order to protect against spam and other automated abuse. The reCAPTCHA tool may make use of cookies, as well as other information like IP address, date, time, language, screen size and resolution, and mouse movements, while on the page. The use of the reCAPTCHA service and the treatment of any information collected through the service are subject to Google's applicable privacy policy, available at <https://policies.google.com/privacy>, and Google's terms of service, available at <https://policies.google.com/terms?hl=en>.

9. Information Security

ADP BrightJump is committed to maintaining the appropriate organizational, technical, and physical controls designed to protect Personal Data entrusted to us from anticipated threats and hazards and unauthorized access and use. ADP BrightJump will strive to provide security that is proportional to the sensitivity of the Personal Data being protected. Additional information about ADP's Global Security Organization may be found at <http://www.adp.com/trust>.

10. Data Retention

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).

11. Third Party Services

This Privacy Statement only addresses the use and disclosure of information by ADP BrightJump. This Privacy Statement does not address, and we are not responsible for, the privacy, information, or other practices of any third parties, including any third party operating a website, app, or service to which the ADP BrightJump links. This inclusion of a link does not imply our endorsement of the linked site or services. Our suppliers, business partners, and other third-party websites that may be accessible through ADP BrightJump have their own privacy statements and data collection, use and disclosure practices. We encourage you to familiarize yourself with the privacy statements provided by third parties prior to providing them with information.

ADP BrightJump may provide functionality allowing you to make payments using a third-party payment service with which you have created your own account. When you use such a service to make a payment to us, your Personal Data will be collected by such third party and not by us and will be subject

to the third party's privacy policy, rather than this Privacy Statement. We have no control over, and are not responsible for, any such third party's collection, use or disclosure of your Personal Data.

12. Use by Minors

ADP BrightJump is not directed to individuals under the age of 18 and we do not knowingly collect Personal Data from individuals under 18. We do not sell or "share" (for cross-context behavioral advertising purposes) the Personal Data, including the Sensitive Personal Data, of minors under 18 years of age.

13. Sensitive Data

Subject to your consent where required by applicable law, we collect, use, and disclose Sensitive Personal Data for purposes of performing services for our business, providing goods or services as requested by you, ensuring safety, 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, providing analytic services, providing storage, activities relating to quality or product improvement, and other collection and use that is not for the purpose of inferring characteristics about an individual. We do not use Sensitive Personal Data beyond these purposes.

Unless we request it, we ask that you not send us, and you not disclose, any Sensitive Personal Data (e.g., social security numbers, information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometrics or genetic characteristics or criminal background) on or through the ADP BrightJump or otherwise to us.

14. Communication Preferences

You may limit the information you provide to us. You may also limit the marketing communications that we send to you. To opt-out of marketing emails, simply click the link labeled "unsubscribe" at the bottom of any marketing email we send you. You may also change your communication preferences on the settings page.

Please note that if you are currently receiving services from us and you have decided to opt-out of marketing communications, we may still send you important administrative messages, from which you cannot opt-out.

If you have questions about your choices or if you need assistance with opting out, please contact us via email to privacy@adp.com. You may also write us at the address in the "**How to Contact Us**" section below. If you send us a letter, please provide your name, address, email address, and information about the communications that you do not want to receive.

15. Access, Correction, Erasure, and Other Individual Rights

You may contact brightjump@adp.com to request access to your data, to exercise any of the individual rights afforded to you by us or by applicable data protection laws and regulations. You may also write to us at the address in the "**How to Contact Us**" section below. If you send us a letter, please provide your name, address, email address, and detailed information about the changes you would like to make. We will respond to requests in accordance with applicable data protection laws.

To make an individual rights request for access, correction erasure or other rights, please contact us by completing our webform or by emailing us at brightjump@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.

You may also write to us at the address in the “**How to Contact Us**” section below. If you send us a letter, please provide your name, address, email address, and detailed information about your request. We will respond to requests in accordance with applicable data protection laws.

Additional Individual Rights for US Consumers

US consumers may make the following specific rights requests, subject to applicable US consumer privacy law:

- (a) **Right to Access, Know and Portability** -- You may request to know whether we process your Personal Data and request to access such Personal Data, including, where applicable, a request to obtain a copy of the Personal Data you provided to us in a portable format.

You may also request that we disclose the following information to you:

- (1) The categories of Personal Data we collected and process 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 CCPA) and the categories of third parties with whom we shared such Personal Data; and
- (5) The categories of Personal Data that we disclosed about you to third parties, and the categories of third parties to whom we disclosed such Personal Data (if applicable).
- (6) A list of third parties to whom your Personal Data was disclosed.

- (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 or Targeted Advertising** -- You may request to opt-out of the “sharing” of your Personal Data for purposes of cross-context behavioral or targeted advertising.

To request to opt-out of any future sharing of your Personal Data for purposes of cross-context behavioral or targeted advertising, please go to [ADP.com](https://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.

We also process opt-out preference signals, such as the Global Privacy Control (GPC). The GPC is a mechanism that enables consumers to automatically communicate their privacy preferences to opt-out of sale and sharing of their personal information to this website. This ensures that the consumer's opt-

out preference is honored through compatible browsers or extensions that support GPC, consistently across all websites accessed through the browser or device you are using. Go to your browser's setting to enable GPC. If enabled you will receive notification or see a visual indication (e.g., banner or pop-up message) on our site confirming that your GPC signal has been detected and your opt-out request has been processed. For information about how to use the Global Privacy Control, please visit <https://globalprivacycontrol.org/>.

We will not unlawfully discriminate against you for exercising your rights under applicable US consumer privacy law.

Authorized Agents Submitting a Request on Behalf of a Consumer

You may choose to designate an authorized agent to make a request 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 or confirm that you provided the agent permission to submit the request. Authorized agents may submit their request as detailed above.

Appeal Process

If you are a Colorado, Virginia, Montana, Oregon, Texas, or Connecticut consumer, and we refuse to take action on your request, you may appeal our refusal within a reasonable period after you have received notice of the refusal. You may file an appeal by contacting us via email at brightjump@adp.com.

Nevada Privacy Rights

ADP collects personal information from you in the course of providing requested services. Unless otherwise stated, ADP does not sell any Covered Information, as defined under Nevada law (S.B. 220). If you would like to make a further inquiry regarding the selling of your Covered Information, as defined under Nevada law, please contact privacy@adp.com.

16. How to Contact Us

Please contact us if you have questions regarding this Privacy Statement. You may reach us via email at brightjump@adp.com or via mail at address below. If you send us a letter, please provide your name, address, email address, and detailed information about your question.

ADP Global Data Privacy and Governance Team

MS 325

One ADP Boulevard

Roseland, NJ 07068-1728 USA

17. How to Lodge a Complaint

If you believe that we have not handled your Personal Data properly or that it has breached its privacy obligations, under any applicable data protection laws, you may file your complaint in writing to the address above in the **"How to Contact Us"** section, or via email, to the Global Data Privacy and Governance Team at privacy@adp.com.

The Global Data Privacy and Governance Team will investigate each complaint and notify you within a reasonable timeframe of the outcome of the investigation. If you are not satisfied by the resolution, you may file a complaint or claim with the relevant regulatory authorities or the courts.

18. Changes to this Privacy Statement

From time to time, we may update this Privacy Statement, and we encourage you to review it regularly. If we make changes, we will notify you by revising the date at the top of the statement with a new **“Last Updated”** date. Any changes will become effective when we post the revised Privacy Statement on our sites or within our application. For a printable copy of this Privacy Statement, please go to <https://brightjump.adp.com/public/terms-of-privacy.pdf>