

CALIFORNIA EMPLOYEE AND JOB APPLICANT PRIVACY POLICY

Last Updated: June 24, 2025

This California Employee and Job Applicant Privacy Policy ("Privacy Policy") applies only to employees and job applicants that are residents of the State of California. This Privacy Policy describes how Penta Group, LLC and its affiliates ("we," or "us") collects, uses, discloses, and processes your Personal Information ("you" and "your"). We reserve the right to change this Privacy Policy at any time. If we change our Privacy Policy, we will post an updated version on this website. Please check back periodically to see if our Privacy Policy has been updated. Updates to the Privacy Policy will be referenced by the "Last Updated" date shown above.

1. Definitions.

"Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household. "Personal Information" does not include: (a) publicly available information or lawfully obtained, truthful information that is a matter of public concern; or (b) information that is deidentified or aggregate information.

"Sensitive Personal Information" means Personal Information that reveals information such as: (a) social security, driver's license, state identification card, or passport number; (b) 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; (c) precise geolocation; (d) racial or ethnic origin, religious or philosophical beliefs, or union membership; (e) the contents of an mail, email, and text messages unless we are the intended recipient of the communication; (f) genetic data; and (g) neural data. Sensitive Personal Information includes the processing of biometric information for the purpose of uniquely identifying an individual, Personal Information collected and analyzed concerning an individual's mental or physical health and Personal Information collected and analyzed concerning an individual's sex life or sexual orientation. Sensitive Personal Information that is publicly available is not considered Sensitive Personal Information or Personal Information.

2. Information We Collect, the Categories of Source of Collection and the Purpose for Collection.

Set forth below are the categories of Personal Information we collect and that have collected in the preceding 12 months, the categories of sources from which the Personal Information was collected and the business or commercial purpose for such collection. Please note that we may not collect all of the information referenced below regarding you.

Category of Personal Information	What We Collect	Categories of Sources from which Personal Information Collected	Business Purpose for Collection
PERSONAL INFORMATION			
Identifiers	Real name Alias Postal address Unique personal identifier Online identifier	Directly from you Automatically, such as when you visit our website (e.g., cookies on our websites)* Our service providers	To assess your employment application To manage workforce activities and personnel To maintain your contact information To assist you in case of emergency

	Internet protocol address Email address Account name Social security number Driver's license number Passport number Date of birth Dependent information Beneficiary information		To recruit employees and perform background screening To manage wages and expenses To administer healthcare and other benefits To perform identity verification, accounting, audit, and other internal functions To comply with law or legal process such as tax deductions, reporting, and record-keeping requirements
Any Personal Information described in subdivision (e) of Section 1798.80 of California Civil Code (Not Included In Other Rows).	Signature Characteristics or description Telephone number Insurance policy number Bank account number Credit card number Debit card number Other financial information Medical information Health insurance information	Directly from you Automatically Our service providers	Same as above.
Protected Characteristics	Race Color Sex/gender Pregnancy, childbirth, breastfeeding and/or related medical conditions Gender identity, gender expression Sexual orientation Marital status Medical Condition (genetic characteristics,	Directly from you Our service providers	To comply with demographic reporting requirement For recruitment purposes To design employee retention programs and diversity initiatives To comply with law or legal process, such as tax deductions, reporting, and record-keeping requirements

	cancer or a history of cancer) Military or veteran status National origin Ancestry Disability (mental and physical including HIV/AIDS, cancer, and genetic characteristics) Genetic information Age (over 40) Request for family care leave Request for Pregnancy Disability Leave Retaliation for reporting patient abuse in tax-supported institutions		
Internet Information or Other Electronic Network Activity Information	Electronic network activity information Browsing history Search history Information regarding interaction with a website, application, or advertisement	Directly from you Automatically Our service providers	To manage workforce activities and personnel Operate and manage IT and communications systems and facilities To maintain security on our websites and Internet-connected assets To manage employee programs
Geolocation Data	Internet protocol address	Directly from you Automatically Our service providers	To manage workforce activities and personnel To manage workforce activities and personnel For security purposes
Audiovisual Information	Electronic information (e.g., meeting recordings) Visual information (e.g., camera footage) Thermal information	Directly from you Automatically	To keep record of meetings in case necessary to refer to such information To manage workforce activities and personnel For security purposes

	Olfactory information		
Professional or Employment Information	Professional history Employment history	Directly from you Our service providers	<p>To assess your candidacy as an employee</p> <p>To manage workforce activities and personnel</p> <p>To recruit employees and perform background screening</p> <p>To ensure compliance with work-related licensing and credentialing</p> <p>To facilitate a better, safer, and more efficient working environment</p> <p>To monitor, investigate, prevent, and redress potential breaches of applicable policies, regulations, and laws</p> <p>To carry out our obligations and enforce our rights arising from any contracts entered into between you and us</p>
Education Information	Educational history	Directly from you Our service providers	See previous row
<p>Inferences</p> <p>Note: This includes inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes</p>	Job evaluation information	Directly from you	Employee assessments
SENSITIVE PERSONAL INFORMATION			
Sensitive Personal Identifiers	Social security number Driver's license number	Consumer reporting agencies Service providers	<p>To recruit employees and perform background screening</p> <p>To manage wages and expenses</p>

	State identification card number Passport number	Directly from you	To administer healthcare and other benefits
Account Information	Information required to access your work account	Directly from you	Operate and manage IT and communications systems and facilities To maintain security on our websites and Internet-connected assets
Precise Geolocation	GPS information	Automatically through GPS technology	To manage workforce activities and personnel
Sensitive Protected Characteristics	Racial origin Ethnic origin	Directly from you	To comply with demographic reporting requirement For recruitment purposes To design employee retention programs and diversity initiatives To comply with law or legal process, such as tax deductions, reporting, and record-keeping requirements
Contents of Communications	Information on emails and messages via Teams lives on the network Emails not intended for business purposes made through work email	Directly from you Our service providers Automatically	For security purposes To comply with law or legal process, such as tax deductions, reporting, and record-keeping requirements
Health Information	Medical information (FMLA) Health insurance information Disability Information Other health information	Directly from you Our service providers	To manage safety requirements To administer healthcare and other benefits
Sex Life or Sexual Orientation Information	Sexual Orientation	Directly from you	To comply with demographic reporting requirement For recruitment purposes

			<p>To design employee retention programs and diversity initiatives</p> <p>To comply with law or legal process, such as tax deductions, reporting, and record-keeping requirements</p>
--	--	--	---

*Cookies are small text files that store information on computer or mobile device, and enable websites like ours to capture and remember information about you. We use cookies and other similar technologies to save your website preferences for future visits, allow you to login automatically, and to compile data about your interactions with our website so that we can offer better website experiences and tools in the future.

3. Personal Information We Disclose About You and Its Business Purpose.

We do not sell your Personal Information and we don't share your Personal Information for cross context behavioral advertising.

We disclose your Personal Information only to service providers, vendors, and contractors that perform services on our behalf. When we disclose Personal Information on that basis, we have or will have entered into a contract that prohibits the service provider from using or disclosing that information except where necessary to perform the services for which we have contracted.

The business purposes for which we disclose Personal Information to our service providers, contractors, and vendors include:

- **Security and Fraud Detection:** We may disclose Personal Information for our security and fraud detection services including detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity; and prosecuting those responsible for that activity.
- **Functionality & Debugging:** We may disclose Personal Information to engage in debugging to identify and repair errors that impair existing intended functionality.
- **Services on Our Behalf:** We may disclose Personal Information in order to receive services performed on our behalf, including maintaining or servicing accounts, providing service for employees, processing or fulfilling requests and transactions, verifying employee information, processing payroll, expenses and payments, evaluating and responding to requests, providing storage, or providing similar services on our behalf.

The following chart sets forth the categories of Personal Information we have disclosed to our service providers for a business purpose over the past 12 months.

Categories of Personal Information that We Disclose	Business Purposes for the Disclosure of Personal Information
PERSONAL INFORMATION	
Identifiers	<p>Security and Fraud Detection</p> <p>Functionality & Debugging</p> <p>Services on Our Behalf</p>

Section 1798.80 Identifiers (Not Included in Other Rows)	Security and Fraud Detection Functionality & Debugging Services on Our Behalf
Protected Characteristics	Services on Our Behalf
Internet Information	Security and Fraud Detection Functionality & Debugging Services on Our Behalf
Geolocation Data	Security and Fraud Detection Functionality & Debugging Services on Our Behalf
Audiovisual Information	Services on Our Behalf
Professional or Employment Information	Services on Our Behalf
Education Information	Services on Our Behalf
SENSITIVE PERSONAL INFORMATION	
Sensitive Personal Identifiers	Services on Our Behalf
Account Information	Services on Our Behalf
Precise Geolocation	Services on Our Behalf
Sensitive Protected Characteristics	Services on Our Behalf

As Necessary: We may also disclose Personal Information, as necessary: (a) to comply with any legal process; (b) to respond to requests from public and government authorities; (c) to enforce our terms and conditions; (d) to protect our operations and protect our rights, privacy, safety or property, and/or that of you or others; and (e) to allow us to pursue available remedies or limit the damages that we may sustain. We may also use Personal Information in connection with or during negotiation of any reorganization, acquisition, merger, sale, joint venture, 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).

We only use Sensitive Personal Information for purposes disclosed herein. We do not use or disclose Sensitive Personal Information for purposes other than those specified herein.

4. Our Retention Policy – How Long We Keep Your Personal Information.

We will retain each category of your Personal Information identified above for an amount of time that is reasonably necessary for us to use the information for the purposes disclosed herein and for any other permitted purposes, including retention of Personal Information pursuant to any applicable contract, law or regulation.

To determine the appropriate retention period for Personal Information, we consider the amount, nature, and sensitivity of the Personal Information, the potential risk of harm from unauthorized use or disclosure of your Personal Information, the purposes for which we process your Personal Information and whether we can achieve those purposes through other means, and the applicable legal requirements.

5. Your Rights if You Are a Resident of California.

California residents may exercise certain privacy rights pursuant to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2023, and related regulations. Your right to submit certain requests as a California resident are described below. Please note that these rights are subject to certain exceptions and certain of these rights are subject to verification mechanisms.

- Right to Know Personal Information Collected About You. You have the right to know: (1) the categories of Personal Information we have collected about you; (2) the categories of sources from which the Personal Information is collected; (3) the business or commercial purpose for collecting Personal Information; (4) the categories of third parties to whom we disclose Personal Information; and (5) the specific pieces of Personal Information we have collected about you. You also have the right to know the list of all third parties to whom we have disclosed Personal Information, as defined under California Civil Code Section 1798.83(e) (a/k/a the “Shine the Light Law”), during the preceding year for third-party direct marketing purposes. You may submit a request by calling us at 888-275-2173 or emailing us at info@pentagroup.co.
- Right to Know Personal Information Disclosed, Sold or Shared and to Whom. You have the right to request that we disclose to you: (1) the categories of Personal Information that we collected about you; and (2) the categories of Personal Information that we disclosed about you for a business purpose and the categories of persons to whom it was disclosed for a business purpose. You may submit a request by calling us at 888-275-2173 or emailing us at info@pentagroup.co.
- Right to Request Deletion of Your Personal Information. You have the right to request that we delete your Personal Information, subject to a number of exceptions. Following receipt of a request, we will let you know what, if any, Personal Information we can delete from our records. If we cannot delete all of your Personal Information, we will let you know the reason. You may submit a request by calling us at 888-275-2173 or emailing us at info@pentagroup.co.
- Right to Correct Inaccurate Information. If you believe that any of the Personal Information we maintain about you is inaccurate, you have the right to submit a request for us to correct that information. Upon receipt of a request, we will use commercially reasonable efforts to correct the information as you direct. You may submit a request by calling us at 888-275-2173 or emailing us at info@pentagroup.co.
- Right to Opt-Out of the Sale and Sharing of Your Personal Information. Since we do not sell your Personal Information and do not share it for cross-context behavioral advertising, this right does not apply to you.
- Right to Limit the Use of Your Sensitive Personal Information. Given our data practices regarding your Sensitive Personal Information, this right does not apply to you.
- Right to Non-Discrimination for Exercising Your Rights. If you choose to exercise any of your rights, you have the right to not receive discriminatory treatment by us.

When you make a request to know, delete and/or correct, to help protect your privacy and maintain security, we will take steps to verify your identity. Our verification procedure may differ depending on whether you have an account with us or not and the request you are making. The following generally describes the verification processes we use:

- Password Protected Accounts. If you have a password-protected account with us, we may use existing authentication practices to verify your identity but will require re-authentication before disclosing, correcting or deleting data. If we suspect fraudulent or malicious activity relating to your account, we will require further verification (as described below) before complying with a request to know or delete.
- Verification for Non-Accountholders. If you do not have, or cannot access, a password-protected account with us, we will generally verify your identity as follows:

- *For requests to know categories of Personal Information*, we will verify your identity to a reasonable degree of certainty by matching at least two data points provided by you with reliable data points maintained by us.
- *For requests to know specific pieces of Personal Information*, we will verify your identity to a reasonably high degree of certainty by matching at least three data points provided by you with reliable data points maintained by us. We will also require a declaration, signed under penalty of perjury, that the person requesting the information is the person whose information is the subject of the request or that person's authorized representative. We will maintain all signed declarations as part of our records.
- *For requests to correct or delete Personal Information*, we will verify your identity to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the Personal Information and the risk of harm posed by unauthorized deletion. We will act in good faith when determining the appropriate standard to apply.

If there is no reasonable method by which we can verify your identity, we will state so in response to a request to know or delete Personal Information, including an explanation of why we have no reasonable method to verify your identity.

If you use an authorized agent to submit a request to know, delete or correct, we may require the authorized agent to provide proof that you gave the agent signed permission to submit the request. We may also require you to do either of the following: (a) verify your own identity directly with us; or (b) directly confirm with us that you provided the authorized agent permission to submit the request. This requirement does not apply if you have provided the authorized agent with power of attorney pursuant to California Probate Code sections 4121 to 4130.

We will respond to requests to know, requests to delete and / or delete no later than 45 calendar days. If we cannot verify your request within 45 days, we may deny your request. If necessary, we may take up to an additional 45 days to respond to your request but in such an event will provide you a notice and an explanation of the reason that we will take more than 45 days to respond to your request.

6. How to Contact Us.

If you have any questions or concerns about our privacy policies and practices, please feel free to contact us by calling us at 888-275-2173, emailing us at info@pentagroup.com or by mail at 1666 K Street NW, Suite 500, Washington, DC 20006.