

APPLICANT AND EMPLOYEE PRIVACY NOTICE FOR CALIFORNIA RESIDENTS

Effective Date: January 3, 2024

Last Updated: September 3, 2024

This Privacy Notice applies solely to applicants and employees of Envita Solutions, LLC and its subsidiaries and affiliates (“we,” “us,” “our,” or “Company”) who reside in the State of California (“you”). We adopt this notice to comply with the California Consumer Privacy Act of 2018 and California Privacy Act of 2020 (collectively, the “CCPA”), as amended, and its implementing regulations.

Assistance for Disabled Employees

Alternative formats of this Privacy Notice are available to individuals with a disability. Please contact Employee Hub at EmployeeHub@thgrp.com or 1-800-303-0408 for assistance.

Definition Specific to this Privacy Notice

“**Personal Information**” under the CCPA 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 consumer/employee or household. Personal Information does not include publicly available information obtained from government records; deidentified or aggregated consumer information that cannot be reconstructed to identify you; any information covered under the Gramm-Leach-Bliley Act or the California Financial Information Privacy Act, activities covered by the Fair Credit Reporting Act, or protected health information as defined under the Health Insurance Portability and Accountability Act. Personal Information includes Sensitive Personal Information.

“**Sensitive Personal Information**” under the CCPA includes Personal Information that reveals, among other things, social security number, driver’s license number, state identification card number, passport number, racial or ethnic origin, union membership, or the contents of a Consumer’s mail, email, and text messages, unless the Company is the intended recipient of the communication. Sensitive Personal Information also includes information concerning the Applicant or Employee’s health, sex life, or sexual orientation.

The Personal Information We Collect

Stated below are the categories of Personal Information we collect about you in the employee context; examples of the type of Personal Information in each category; and the business purpose(s) for which that category of Personal Information is collected in the employee context.

<u>Category of Personal Information</u>	<u>Examples</u>
Unique identifiers	Name, signature, address, telephone email, account name, SSN, DL number, passport number, online identifier, IP address.
Government ID number	Social security number, passport number, driver’s license or state identification card number.

Physical description	Physical characteristics or description.
Financial information	Bank account number, credit card number, debit card number, or any other financial information.
Health/medical information	Medical information or health insurance information.
Biometric data	Fingerprints, facial scans, eye scans, voice recognition, typing cadence, and any other biometric identifier that we may use for security, other operational purposes, or our voluntary wellness program.
Insurance information	Insurance policy number, health insurance information.
Protected class data	Characteristics of protected classifications under California or federal law, including: race, ancestry, national origin, age (40 years or older), marital status, sex, sexual orientation, physical or mental health conditions, disability, genetics, marital status, and veteran or military status.
Internet activity	Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and use of our information technology resources.
Geolocation data	GPS coordinates, location-tracking information, physical location or movements.
Employment information	Professional or employment-related information.
Education information	Personally identifiable education information that is not publicly available (e.g. grades, financial aid).
Audiovisual Information	On-site security cameras, pictures, video and audio recordings.
Inferences	Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
Sensitive Personal Information	Including: <ul style="list-style-type: none"> a. Personal Information that reveals: <ul style="list-style-type: none"> i. Social security, driver's license, state identification card, or passport number; ii. Account log-in, financial account number, debit card number, or credit

	<p>card number in combination with any required security or access code, password, or credentials for allowing access to an account;</p> <ul style="list-style-type: none"> iii. Precise geolocation; iv. Racial or ethnic origin, religious or philosophical beliefs, or union membership; v. Contents of a Consumer’s email and text messages, unless the business is the intended recipient thereof; or vi. Genetic data. <ul style="list-style-type: none"> b. Biometric data processed for the purpose of uniquely identifying a Consumer; c. Personal Information Collected and analyzed concerning a Consumer’s health; and d. Personal Information Collected and analyzed concerning a Consumer’s sex life or sexual orientation.
--	--

The Use of Personal Information

We may use or disclose the personal information we collect that is described above for one or more of the following purposes:

- **Workforce Management**, including but not limited to, the following uses:
 - To evaluate individuals for a position with us when applying for a position or we receive the individual's information related to a position with our companies
 - To comply with state and federal laws requiring employers to maintain certain records
 - To process payroll and manage applicable tax withholding and reporting
 - To administer and maintain group health insurance benefits, additional wellness programs, 401(k) and/or retirement plans, life insurance, disability insurance, leave programs and additional fringe benefit programs
 - To manage and/or analyze all aspects of employee performance of their job duties and employment, including, but not limited to, training, talent management, periodic reviews, performance tracking, promotions, and discipline
 - For surveys, research, analysis and strategic development to implement, maintain and promote an engaging work experience with the company
 - To review and audit employee interactions with the company’s customers and business partners
 - For employee and facility security
 - To support information technology services to the workforce
 - To facilitate remote work and to communicate with employees working remotely
 - For emergency training and emergency response
 - To conduct internal audits and workplace investigations

- Monitor, investigate, and enforce compliance with and potential breaches of the Company's policies and procedures
- Otherwise accomplish our business purpose and objectives
- **Detecting and Protecting** including but not limited to, the following uses:
 - Detecting and protecting against security incidents and malicious, deceptive, fraudulent or illegal activity, or violations of the company's policies or the law
 - For fraud and crime prevention
 - For information protection and cybersecurity
- **Legal/Compliance/Regulatory** including but not limited to, the following uses:
 - To meet additional legal, compliance, and regulatory requirements
 - To defend the company's rights and property
- **Backups and Archives** including but not limited to, the following uses:
 - For disaster recovery, business continuity and record keeping obligations

We may disclose your Personal Information to our Service Providers for the purposes described above only to the extent needed for them to perform their functions, and require them to protect the confidentiality and security of such information. We may disclose your Personal Information to our Third Parties at your direction, for a business purpose, or to government authorities, including regulatory agencies and courts, as reasonably necessary for our business operational purposes, to assert and defend legal claims, and otherwise as permitted or required by law.

Your Data Subject Rights

As an Applicant or Employee, you have the following rights regarding our Collection and use of your Personal Information, subject to certain exceptions:

- **Right to Receive Information on Privacy Practices.** We have provided such information in this Policy, and you may request further information about our privacy practices by contacting us as at the contact information provided below.
- **Right to Deletion:** You may request that we delete any Personal Information about you we that we collected from you.
- **Right to Correction:** You may request that we correct any inaccurate Personal Information we maintain about you.
- **Right to Know:** You may request that we provide you with the information about how we have handled your Personal Information in the 12 months preceding your request.
- **Right to Receive Information About Onward Disclosures:** You may request that we disclose to you the categories of Personal Information that we have disclosed, Sold or Shared about you, the categories of persons to whom we disclosed your Personal Information, and the categories of Third Parties to whom the Personal Information was Sold or Shared.

- **Right to Opt-Out of the Sale and Sharing of Your Personal Information and to Limit the Use of Your Sensitive Personal Information:** You have the right to opt-out of the Sale and Sharing of your Personal Information. You also have the right to limit the use of your Sensitive Personal Information to the purposes authorized by the CCPA.
 - We do not Sell or Share Personal Information. Further, we do not use Sensitive Personal Information for purposes beyond those authorized by the CCPA. Relatedly, we do not have actual knowledge that we Sell or Share Personal Information of California Consumers under 16 years of age. For purposes of the CCPA, a “Sale” is the disclosure of Personal Information to a Third Party for monetary or other valuable consideration, and a “Share” is the disclosure of Personal Information to a Third Party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.
- **Right to Non-Discrimination:** You have the right not to be discriminated against for exercising your data subject rights. We will not discriminate against you for exercising your data subject rights.

Retention of Personal Information

We retain each of the above-listed categories of Personal Information for the duration of your Applicant and/or Employee relationship with us, as applicable, and longer as may be required by applicable laws or necessary for our legitimate business purposes.

Additional Information

If you would like additional information regarding this Privacy Notice, please contact Employee Hub at EmployeeHub@thgrp.com or 1-800-303-0408 for assistance. We may ask you to provide information that will enable us to verify your identity in order to comply with your data subject request. In particular, if you authorize an agent to make a request on your behalf, we may require the agent to provide proof of signed permission from you to submit the request, or we may require you to verify your own identity to us or confirm with us that you provided the agent with permission to submit the request. In some instances, we may decline to honor your request if an exception applies under the CCPA. We will respond to your request consistent with applicable law.

Changes to this Privacy Notice

Company reserves the right to amend this Privacy Notice at our discretion and at any time, consistent with the CCPA and California law. If we make changes to this Privacy Notice, we will notify you by posting an updated notice on <https://myheritagegroup.com/thg/policies/envita-solutions>.