

Notice of Collection and Privacy Notice for California Employees

- [Introduction](#)
- [Collection of Personal Information](#)
- [Sources of Personal Information](#)
- [Use of Personal Information](#)
- [Disclosure of Personal Information; No Sale](#)
- [Sharing of Personal Information](#)
- [Your Rights](#)
- [Retention](#)
- [Accessibility](#)
- [Changes to this Notice and Effective Date of Notice](#)
- [Contact Information](#)

Introduction

This Notice of Collection and Privacy Notice for California Employees (“**Notice**”) applies solely to current and former employees of the Company, dependents and beneficiaries of Employees, and emergency contacts for Employees, who reside in the state of California (each, a “Resident,” and collectively, “Residents”). The Company has adopted this Notice to comply with the California Privacy Rights Act of 2020 (“**CPRA**”). Any terms defined in the CPRA have the same meaning when used in this Notice.

This Notice supplements the Hilltop Global Employee Privacy Policy (“**Employee Privacy Policy**”). The terms “Employee” and “Hilltop” have the meanings given to them in the Employee Privacy Policy.

Collection of Personal information

The Company collects “**Personal Information**,” meaning information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Resident. However, the term “**Personal Information**” excludes the following information as provided by the CPRA:

1. Publicly available information from government records.
2. De-identified or aggregated consumer information.
3. Information excluded from the CPRA’s scope, including health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data; and Personal Information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver’s Privacy Protection Act of 1994.

The Company has collected the following Personal Information from Residents within the last twelve (12) months as outlined below:

1. **Identifiers** including a real name, alias, signature, postal address, unique personal identifier, online identifier, Internet Protocol Address, email address, telephone number, account name, Social Security number, driver’s license number, passport number, financial information, benefit

plan enrollment, physical characteristics or description, medical information, leave of absence information, insurance policy number, educational information, employment, current or past employment and salary history, performance evaluations, emergency contact information, family details, sensory data, including audio or visual information, background check and criminal history, work authorization, or other similar identifiers.

2. **Protected Classifications Characteristics under California or Federal Law** including age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, and genetic information (including familiar genetic information).
3. **Commercial information**, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
4. **Biometric Information** including fingerprint scans and related information and certain wellness metrics.
5. **Internet or Other Similar Network Activity** including activity on the Company's information systems, such as internet browsing history, search history, intranet activity, email communications, social media posting, stored documents and emails, and usernames and passwords. It also includes activity on communications systems, including phone calls, call logs, voice mails, text messages, chat logs, app use, mobile browsing and search history, mobile email communications, and other information regarding an Employee's use of company-issued devices.
6. **Geolocation Data**, including physical location or movements, including physical address information that Residents provide to the Company to receive correspondence and documents from the Company and GPS location data from Company-issued mobile devices or Company-owned vehicles.
7. **Audio, electronic, visual, thermal, olfactory, or similar information**, including voice recordings from phone calls, recorded video conferences, photos for ID badges, and video recordings from security cameras.
8. **Professional or employment-related information**, including past employers and job titles, educational information, employment restrictions (such as non-compete, non-solicitation, or immigration status), litigation history, regulatory violations, disciplinary actions (such as by a professional organization), and information provided by recruiters.
9. **Inferences Drawn from Other Personal Information**, including a profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
10. **Sensitive personal information**, such as your 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, or union membership; the contents of your mail, email and text messages, unless the Company is the intended recipient of the communication; your genetic data; the processing of biometric Information for the purpose of uniquely identifying you; health information; information

concerning your sex life or sexual orientation. Sensitive personal information is not considered Sensitive Personal Information if it is publicly available.

Sources of Personal information

The Company obtains this category of Personal Information from the following categories of sources:

1. Directly from you or your agents. For example, from documents or information you provide to us or from an employment agency or recruiter.
2. Indirectly from you or your agents. For example, through the information that we collect from you or your agents in the course of administering our relationship with you as an Employee, including from background check providers, occupational health and other health providers, pension administrators, and other Employee benefits providers.
3. Directly or indirectly from your activities on our IT and communications systems and networks when you engage with them as an Employee.
4. From third parties that interact with us in connection with the services we perform.
5. From our affiliates and subsidiaries.
6. From third-party data aggregators.
7. From CCTV images or security images and/or video from our landlords or taken using our own systems

Use of Personal information

The Company may use or disclose the Personal Information it collects from the categories above for the following purposes, as further detailed in the Employee Privacy Policy:

1. To perform the services or provide the goods reasonably expected by you if you request those goods or services from the Company, such as to administer benefits for you and your household.
2. To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted Personal Information, provided that the use of your Personal Information is reasonably necessary and proportionate for this purpose.
3. To resist malicious, deceptive, fraudulent, or illegal actions directed at the Company and its affiliates and to prosecute those responsible for those actions, provided that the use of your Personal Information is reasonably necessary and proportionate for this purpose.
4. To ensure the physical safety of natural persons, provided that the use of your Personal Information is reasonably necessary and proportionate for this purpose.
5. For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the Company, provided that the Personal Information is not disclosed to another third party and is not used to build a profile about you or otherwise alter your experience outside of your current interaction with the Company as an Employee.
6. To perform services on behalf of the Company, provided that the use of your Personal Information is reasonably necessary and proportionate for this purpose.

7. To verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the Company, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the Company, provided that the use of your personal information is reasonably necessary and proportionate for this purpose.
8. For purposes that infer characteristics about you (except that we do not use Sensitive Personal Information for this purpose).

Disclosure of Personal Information, No Sale

Presently, Hilltop does not sell and has not sold any personal information for monetary value in the past 12 months, nor do we intend to sell, rent, or share your personal information with third parties that are not affiliated with or providing services to Hilltop.

Sharing of Personal Information

In the preceding twelve (12) months, the Company has disclosed Personal Information to the following categories of third parties for a business purpose:

1. Service providers, such as background check vendors, third-party human resources vendors, information technology vendors, and outside legal counsel.
2. State and federal governmental agencies.
3. Third parties to whom Residents or their agent has directed or authorized the Company to disclose Personal Information.

Your Rights

Subject to certain limitations and exceptions, California Residents have the following rights:

- **Right to Know:** You have a right to request information from the Company regarding the Personal Information we collect and disclose for business purposes about you.
- **Deletion:** In certain circumstances, you have the right to request that we delete the Personal Information we collected from you. The right to request deletion is subject to certain exceptions under the CPRA.
- **Limit:** In certain circumstances, you have the right to limit the use and disclosure of your sensitive personal information as set forth in Civil Code section 1798.121.
- **Non-Discrimination:** The Company will not discriminate against Residents for exercising their rights under the CPRA.

How to Submit a Verifiable Request

Consistent with applicable law, you may exercise the rights described above by submitting a request for a copy of the information collected about you in the last 12 months or request deletion of the information if we can verify that you are indeed the individual submitting the request.

You may designate an authorized agent to submit a request on your behalf to access or delete your personal information. To do so, you must: (1) provide that authorized agent written and signed permission to submit such request; and (2) verify your own identity directly with us. Please note that we may deny a

request from an authorized agent that does not submit proof that you have authorized them to act on your behalf.

Retention

Typically, we retain your Personal Information for the period necessary to fulfill the purposes outlined in this Notice unless a longer retention period is required or permitted by law. Please note that in many situations, we must retain all, or a portion, of your Personal Information to comply with our legal obligations, resolve disputes, enforce our agreements, protect against fraudulent, deceptive, or illegal activity, or for another one of our business purposes.

Accessibility

We are committed to ensuring this Notice is accessible to individuals with disabilities. If you wish to access this Notice in an alternative format, please get in touch with us as described in the [Contact Us](#) section below.

Changes to this Notice and Effective Date of Notice

The Company reserves the right to amend this Notice at the Company's discretion and at any time. When the Company makes changes to this Notice, the Company will submit the updated notice to you directly by email using your Company email address or other applicable email address (for independent contractors and Company employees and their dependents/emergency contacts) or by posting the updated Notice on the Company's applicable website or application and updating the Notice's effective date.

Contact Information

If you have any questions or comments about this Notice or how the Company collects and uses your Personal Information as described above, please do not hesitate to contact the Company at:

Phone: 214-525-9196

Email: hilltophr@hilltop-holdings.com

Postal Address: 6565 Hillcrest Avenue, Dallas, TX 75205