UPI

Employee Privacy Policy

UPI ("Company", "we", or "us") collects various types of personal information and sensitive personal information for business purposes. It is our policy to use such information responsibly and to maintain appropriate security measures to keep the information private.

This Privacy Policy describes the types of personal information and sensitive personal information we may collect from our employees, temporary workers, job applicants, and contractors ("individual", "individuals", or "you") and our practices for using, disclosing, and protecting such information.

1. What Is Personal Information?

"Personal information" means information that identifies, relates to, describes, references, or is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual. For purposes of this Privacy Policy, personal information does not include:

- Publicly available information (or lawfully obtained, truthful information that is a matter of public concern;
    - "Publicly available" means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience
- De-identified or aggregated information (i.e., information that cannot be associated with or tracked back to a specific individual); or
- Information excluded from the scope of the California Consumer Privacy Act, such as:
    - 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.

Personal information may also include "sensitive personal information," which means personal information revealing an individual's social security, driver's license, state identification card, or passport number; an individual's 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; an individual's precise geolocation; an individual's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership; the contents of an individual's mail, email, and text messages unless UPI is the intended recipient of the communication; an individual's genetic data; processing biometric information to uniquely identify an individual; personal information collected and analyzed concerning an individual's health; or personal information collected and analyzed concerning a consumer's sex life or sexual orientation. For purposes of this Privacy Policy, sensitive personal information does not include:

- Sensitive personal information that is "publicly available," as explained above.

2. What Personal Information Do We Collect?

The personal information we collect varies based on the type of relationship or interaction we have with a particular individual. The following list sets forth the categories of personal information that UPI may collect. Not all of the categories and examples are applicable to every individual.

- *Identifiers and information protected by California Civil Code section 1798.80(e)*, such as real name, alias, postal address, unique personal identifier, online identifier, internet protocol ("IP") address, email address, account name and password, social security number, driver's license number, passport number, state identification card number, social media handle, or other similar identifiers;

- *Protected class and demographic information*, such as physical characteristics or descriptions, race, gender, age, disability, and national origin of the individual, as well as the individual's spouse and children;

- *Commercial information*, such as records of personal property, products or services purchased or obtained, or other purchasing or consuming histories or tendencies;

- *Biometric information*, such as an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity—this includes but is not limited to imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template,

or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information;

- *Internet and other network activity information*, such as browsing history, search history, IP address, cookies and similar IDs, and information regarding your interaction with an internet website, application or advertisement;

- *Geolocation data*, such as physical locations and movements (e.g., facility entry/exit information);

- *Sensory data*, such as audio, electronic, visual, thermal, olfactory or similar information (e.g., call recordings and security camera footage);

- *Professional or employment-related information*, such as resumes, employment and education history, professional memberships, board service, licenses and certifications, training records, interview notes, payroll information, job titles, work locations, job descriptions, years of service, recruitment details, termination details, attendance records, accident reports, performance reviews, communications, and other human resources related records;

- *Non-public education information* as defined in Family Educational Rights and Privacy Act, such as grades, transcripts, class lists, student schedules, student financial information, or other non-public records maintained by an educational institution or a party acting on its behalf; and

- *Inferences*, such as inferences drawn from any of the above information to create a profile reflecting an individual's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and/or aptitudes.

The sensitive personal information we collect varies based on the type of relationship or interaction we have with a particular individual. The following list sets forth the categories of personal information that UPI may collect. Not all of the categories and examples are applicable to every individual.

- *Government identifiers*, such as social security, driver's license, state identification card, or passport number;

- *Complete account access credentials* for any accounts related to your job application, employee onboarding process, selection of your benefits as an employee, or your employment;

- *Precise geolocation*;

- *Racial or ethnic origin*;
- *Citizenship or immigration status*;
- *Religious or philosophical beliefs*;
- *Union membership (to the extent permitted by law if such information is not confidential)*;
- *Mail, email, or text message contents* not directed to UPI but sent from UPI accounts or equipment;
- *Unique identifying biometric information*, such as fingerprints, facial pictures for ID badges and voice recordings on various voicemail messages outgoing and coming, and any images of faces from video surveillance;
- *Health, sex life, or sexual orientation information* such as health conditions, if relevant to your employment, job restrictions, workplace accident and illness information, and health insurance policy information.

3. How Do We Obtain Personal Information?

We obtain personal information from the following categories of sources:

- *Directly from you*, such as when you complete our forms, register for information or services, engage in transactions, communicate with us by telephone, email, text or other means, or otherwise deliver information to us;
- *Indirectly from you,* such as when your computer or mobile device transmits information while interacting with our websites or mobile applications; and
- *From third parties*, such as affiliates, business partners, vendors, service providers, government agencies, or others who support or assess our business.

4. How Do We Use Personal Information?

We may use personal information for a variety of business purposes, including (without limitation) the following:

- Determining eligibility for initial employment;
- Managing the employment relationship;
- Administering pay and benefits;

- Processing work-related claims (e.g. workers' compensation);
- Managing internal business operations;
- Implementing workforce training and development programs;
- Conducting performance reviews and determining performance requirements;
- Assessing qualifications for a particular job or task;
- Supporting information technology (e.g., system maintenance and bug fixes, firewall monitoring, anti-spam and virus protection);
- Succession planning;
- Gathering evidence for disciplinary action or termination;
- Establishing emergency contacts;
- Compiling and managing internal business directories;
- Marketing UPI's products;
- Ensuring the security of company-held information;
- Protecting human health and the environment;
- Monitoring, investigating and enforcing compliance with UPI's policies and procedures;
- Complying with applicable laws and regulations, including (without limitation) tax, health and safety, anti-discrimination, immigration, labor and employment, and social welfare laws;
- Complying with civil, criminal, judicial and regulatory inquiries, investigations, subpoenas or summons;
- Exercising or defending the legal rights of UPI; and
- For any other purpose disclosed by us when you provide the information.

The Company maintains a series of tables containing the personal information and sensitive personal information categories that it collects, along with category-by-category explanations of how the Company uses each category of information. Those tables may be found within our CCPA and CPRA Notice at Collection for California Employees and Applicants, which you may find by visiting: ussupi.com.

5. When and to Whom Do We Disclose Personal Information?

In the preceding twelve (12) months, UPI has not sold any personal information, and except in connection with a business transfer (i.e., a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of UPI's assets) we will not sell your personal information without providing you with an opportunity to opt-out of such sales.

However, we may disclose your personal information to third parties for business purposes. The categories of third parties with whom we share personal information include (without limitation) the following:

- Affiliates, business partners, service providers, government agencies, or other third parties who support or assess our business (e.g., payment processing, workplace and data security, medical care, recruitment and training, IT systems and support, audits, legal compliance);
- A buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of UPI's assets; and
- Any other individual or organization as reasonably necessary to do the following:
    - Monitor, investigate and enforce compliance with UPI's policies and procedures;
    - Comply with applicable laws and regulations, including without limitation applicable tax, health and safety, anti-discrimination, immigration, labor and employment, and social welfare laws;
    - Comply with civil, criminal, judicial or regulatory inquiries, investigations, subpoenas or summons; or
    - Exercise or defend the legal rights of UPI, its employees, owners, directors, officers, contractors, business partners and/or agents.

The Company maintains a series of tables containing the personal information and sensitive personal information categories that it collects, along with category-by-category explanations of how the Company uses each category of information. Those tables may be found within our

CCPA and CPRA Notice at Collection for California Employees and Applicants, which you may find by visiting: ussupi.com.

6. How Do We Protect Personal Information?

UPI endeavors to maintain physical, technical and procedural safeguards that are appropriate to the sensitivity of the personal information in question. These safeguards are designed to protect your personal information and sensitive personal information from loss and unauthorized access, copying, use, modification or disclosure. When appropriate, we enter into contracts requiring the recipients of personal information and sensitive personal information to keep that information confidential and only use it for its intended purpose. Despite these safeguards, no method of data storage or transmission is fully secure.

7. How Long Do We Retain Personal Information?

Except as otherwise permitted or required by applicable law or regulatory requirements, UPI endeavors to retain your personal information and sensitive personal information only for as long as we believe it is necessary to fulfill the purposes for which it was collected.

The intended retention periods for each category of collected personal information or sensitive personal information, or the criteria for determining such a retention period, may be found within a series of tables within our CCPA and CPRA Notice at Collection for California Employees and Applicants, which you may find by visiting: ussupi.com. The intended retention period for each category of personal information and sensitive personal information is as follows: long enough to consider a job applicant for employment with UPI (which is typically for a number of months but could be longer); during an employee's employment and after their employment as needed to for UPI to consider re-hiring or future employment possibilities; and to comply with local, state, and federal law, meaning no less than four years from date of employment application or termination of employment under current law and longer if any relevant litigation is ongoing or new laws are enacted.

8. Your Rights.

Right to Know and Data Portability

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months (the "right to know"). Once we receive your request and confirm your identity (see Exercising Your Rights to Know or Delete further below), we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting or selling that personal information.
- The categories of third parties with whom we share that personal information.
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:
    - sales, identifying the personal information categories that each category of recipient purchased; and
    - disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.
- The specific pieces of personal information we collected about you (also called a data portability request).

Right to Delete

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions (the "right to delete"). Once we receive your request and confirm your identity (see Exercising Your Rights to Know or Delete below), we will review your request to see if an exception allowing us to retain the information applies. We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

- Complete the transaction or process for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing employment relationship with you, or fulfill the requirements of local, state, or federal law, or otherwise perform our contract with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Debug products to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.).
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.

- Enable solely internal uses that are reasonably aligned with individual expectations based on your employment relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

We will delete or deidentify personal information not subject to one of these exceptions from our records and will direct our service providers to take similar action.

Right to Correct

You have the right to request UPI, if it maintains inaccurate personal information about you, to correct the inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.

Right to Limit the Use or Disclosure of Your Sensitive Personal Information

You have the right to limit the use or disclosure of your sensitive personal information to the following uses:

- To perform services or provide goods that an average individual requesting those goods or services would reasonably expect;
- To help ensure security and integrity, if that use is reasonably necessary and proportionate;
- For short term, transient use
- To perform services on behalf of UPI, including maintaining or servicing accounts, providing customer or employee services, processing or fulfilling orders and transactions, verifying customer or employee information, processing payments, providing financing, providing analytic services, providing storage, providing employee benefits, or providing similar services on behalf of UPI;
- To undertake activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by UPI, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by UPI; and
- As authorized by regulations adopted under subparagraph (C) of paragraph (19) of subdivision (a) of California Civil Code Section 1798.185.

Please note that any sensitive personal information that is collected or processed without the purpose of inferring characteristics about you is not subject to this right to limit use and disclosure.

Exercising Your Rights to Know, Delete, Correct, or Limit Use or Disclosure of Sensitive Personal Information

To exercise your rights to know, delete, correct, or to limit the use or disclosure of sensitive personal information as described above, please submit a request in by telephone or by writing (including by email) USS-UPI, Privacy Officer, P.O. Box 471, Pittsburg, CA 94565.

Only you, or someone legally authorized to act on your behalf, may make a request related to your personal information. To designate an authorized agent, you may designate such an agent through writing to the Legal Department, whose contact information appears at the end of this policy. We may require a response from you by contacting you in person, by phone, by email, or by contact information you have provided to us in your employment context to confirm your designation of such an agent.

You may only submit a request to know twice within a 12-month period. Your request to know, delete, correct, or limit use or disclosure of sensitive personal information must::

- Provide sufficient information that allows us to reasonably verify you are an employee about whom we collected personal information or an authorized representative or an authorized representative, subject to our confirmation of this information.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

We will only use personal information provided in the request to verify the requestor’s identity or authority to make it.

Response Timing and Format

We will confirm receipt of your request within ten (10) business days. If you do not receive confirmation within the 10-day timeframe, please contact Human Resources.

We endeavor to substantively respond to a verifiable employee request within forty-five (45) days of its receipt. If we require more time (up to another 45 days), we will inform you of the reason and extension period in writing.

We will deliver our written response by mail or electronically.

Any disclosures we provide will only cover the 12-month period preceding receipt of your request. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance, specifically in Adobe, Microsoft Excel, and/or Microsoft Word or other word processing file formats.

Provided we receive a verifiable employee request to correct inaccurate personal information, we will use commercially reasonable efforts to correct that information as directed by you and required under law.

We do not charge a fee to process or respond to your verifiable employee request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee , we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Non-Discrimination and No Retaliation

We will not discriminate against you or retaliate against you for exercising any of your rights conferred by the California Consumer Privacy Act or California Privacy Rights Act.

9. Changes to This Privacy Policy

We reserve the right to amend this Privacy Policy at our discretion and at any time. When we make changes to this Privacy Policy, we will post the updated policy on UPI's intranet site and update the policy's effective date.

Until and unless we provide you additional notice through an amended Privacy Policy, we will not collect additional categories of personal information or use the personal information for purposes that are materially different from or incompatible with those described in this document.

10. Contact Information

If you have any questions or comments about this Privacy Policy, the ways in which we collect and use your personal information, or your choices and rights regarding such use, please contact the USS-UPI Privacy Officer at:

USS-UPI, LLC
Attn: Privacy Officer
900 Loveridge Road, MS 29
Pittsburg, CA 94565

Fax: (925) 439-6179
Email: legal1@ussupi.com
Toll-Free Phone Number: (800) 877-7672