



## TEEMA HQ California Privacy Rights Policy

Procedure Naming Convention	Procedure Original Date	Procedure Revision Date	Version
Your California Privacy Rights	Dec 16, 2020	May 15, 2024	V4

### PURPOSE

The California Privacy Rights Act (CPRA) enhances privacy rights and consumer protection for residents of California, building on the groundwork laid by its predecessor, the California Consumer Privacy Act (CCPA). The purpose of CPRA is to provide consumers with greater control over their personal information, including the right to know about and decide how their data is used, shared, or sold. It introduces stricter data protection measures, transparency requirements, and the establishment of the California Privacy Protection Agency to enforce privacy laws.

### POLICY

Under California law, California residents have the right to request certain information regarding the disclosure of their personal information to third parties for direct marketing purposes. If we have disclosed any personal information to third parties for such purposes, we will provide a list of the categories of personal information, along with the names and addresses of these third parties, upon request. **To make such a request, please contact us using the request form linked [here](#) or contact us using the toll free number 833-698-3362 or [email us](#).** This request may be made no more than twice in a 12-month period. We reserve the right not to respond to requests submitted other than to the specified email, toll free phone number or through webform. Please include "California Privacy Rights- Request" in the email subject line and in the body of your request. You must provide us with specific information about yourself so that we can accurately respond to the request.

#### California Minors Under 18:

California residents under the age of 18 and registered users of our Online Services may request the removal of content they have posted to our Online Services that can be accessed by any other user. To request removal of content, please contact us using the information provided in the "Contact Us" section of this Policy. When making a request, please provide a description of the content and its location on our Online Services, along with any other information we may require to consider your request. Please note that removal of content does not ensure complete or comprehensive removal of the content or information posted on our Online Services by you.

#### State Consumer Privacy Notice (CA):

This State Consumer Privacy Notice applies to residents of California and sets forth their rights under their respective state's comprehensive privacy laws. This notice supplements our Privacy Policy and explains what Personal Information (PI) we collect about you, where and from whom we obtain it, why we collect it, and your respective state rights regarding it. If you are a California resident, this notice applies to any PI that we collect about you.

#### PI We Collect and Disclose for Business Purposes:

Below are the types of Personal Information we may collect from you, and examples of each:

- **Identifying Information:** such as your full name, gender, date of birth, marital status, employee ID number, signatures
- **Contact Information:** such as your Email address, telephone number, postal address, and contact information for you and for your referrals, references, or emergency contacts.
- **National Identifiers:** such as your SSN, Driver's License Number, passport and visa information and immigration status and documentation.
- **Dependents' Information:** such as your dependents' and their respective names, address, date of birth and Social Security Number (SSN).
- **Educational and Professional Background:** such as your work history, resume/CV, academic and professional qualifications and history, certifications, language proficiencies, awards, security clearance information, and other work-related skills
- **Employment Details:** such as your job title, position, hire dates, base pay, bonus, commission, expense reimbursement, incentive pay and any other wage related information; performance and disciplinary records; timekeeping records including vacation and sick leave records; training records; and personality assessment information that you may take as part of the interview process or while you are an employee.
- **Background Check Information:** such as your background check, credit check, education verification, employment verification, and/or drug testing results (where you have provided consent for such screenings).
- **Benefits Administration Information:** such as your benefits enrollment information, including Dependents' Information you provide.
- **Career Planning Information:** such as your career interests, desired compensation and benefits, desired work location and willingness to relocate, family information you provide as it relates to your career goals or plans, hobbies and interests.
- **Financial Information:** such as your bank account routing and account information, tax information, payroll information and withholdings, and credit card information (for example if you choose to provide it for booking a hotel for work travel).
- **Health and Safety Information:** such as your absence or leave records that contain health-related information (for example information about pregnancy, illness or other medical leaves of absence); information about your health as part of required occupational health screenings or related to a workplace injury; health information related to disability or other accommodation requests; health information related to COVID-19 symptoms, COVID-19 testing results, or COVID-19 vaccination status. Health information we hold about employees is covered by our HIPAA Privacy Notice and not this Notice.
- **Geolocation Information:** such as time and physical location related to your logging into our network or applications or using your badge to enter one of our office locations.
- **Biometric Information:** Your fingerprints (we will collect fingerprints only if we have provided you with a notice prior to collecting it that explains the reason for collection, which is usually for purposes of timekeeping or a security system or healthcare credentialing). If a customer where you will be placed collects fingerprints, we will provide you with that information where we know it, but it is the customer's responsibility to notify you since they are collecting the fingerprint.

- **Characteristics of Protected Classifications under California or Federal Law:** including your race, gender, national origin, disability status and veteran status, where we are required to or permitted to do so by law and in support of equal opportunity monitoring or affirmative action programs.
- **Audio, Visual or Similar Information:** including photos that you provide to us or that you make publicly available on the internet (for example LinkedIn or company/firm websites); and your image from a security camera if you visit one of our locations.
- **Device Information:** Your IP address, browser type and version, browser plug-in types and versions, operating system and platforms of TEEMA ,Electronic Resources (e.g., computers and other devices) you operate.
- **Other Information You Provide:** including any other Personal Information you may elect to provide to us.

We will retain the foregoing categories of PI consistent with our internal record-retention policies and for as long as is necessary to provide products and services to you or as required by law.

**PI does not include:**

- De-identified or aggregated consumer information
- Publicly available information from government records
- Health or medical information covered by HIPAA and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data
- PI covered by other privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994

**Sources Of Personal Information:**

We collect information in a variety of ways:

- **Directly from you.** We collect contact information, identifiers, financial information, commercial information, and professional or employment information that you provide directly to us.
- **When you visit our locations/sites.** When you visit our offices or facilities, we may collect contact information and audio/visual data. We also may collect your activity on our apps and websites.
- **Automatically.** When you access our Sites, we collect identifiers, geolocation data, and internet or electronic usage data using tools like browser cookies
- **From third parties:** We may collect contact information, identifiers, financial information, commercial information, and professional or employment information from third-parties including our vendors, clients, and service providers.
- **From other applicants or consultants.** We may collect contact information, identifiers, financial information, personal characteristics or traits, non-public education information, health

insurance information, medical information, sensitive personal information, and professional or employment information from our current or former applicants or consultants.

- **Social media platforms.** Depending on the publicly available information, information you choose to share and your privacy settings, we may collect contact information, identifiers, audio/visual data, personal characteristics or traits, geolocation data, commercial information, professional or employment information, internet or electronic usage data, and inferences. Based on the way you have set your privacy settings on your social media accounts, most social media platforms, like Facebook and Instagram, analyze data about how you interact with our Sites and combine it with information on other users to provide us information about you. In addition, we may receive information about you if other users interact with us on social media and information about you is visible to us, for example the fact that you are “friends” or other public-facing profile information.

### **Why We Collect PI:**

We collect your PI for one or more of the following business purposes:

- To contact you
- To conduct background checks
- To verify employment eligibility
- To maintain records related to the hiring process
- To respond to an email or particular request from you
- To communicate with you
- To personalize services for you
- To process an application as requested by you
- To administer surveys and promotions
- To provide you with information that we believe may be useful to you
- To perform analytics and to improve our products, websites, and advertising
- To comply with applicable laws, regulations, and legal processes
- To protect someone's health, safety, or welfare
- To protect our rights, the rights of affiliates or related third parties, or take appropriate legal action
- To keep a record of our transactions and communications
- To detect and protect against security incidents
- As otherwise necessary or useful for us to conduct our business, so long as such use is permitted by law

### **How We Share Personal Information:**

We share personal information in the following circumstances or as otherwise described in this Privacy Policy:

- **Service Providers.** We may share personal information with vendors and service providers who support the operation of our services, website, and our business and who need access to such information to carry out their work for us (including, for example, cloud hosting, payment processing, order fulfillment, email delivery, marketing, insurance, operating systems and platforms, transportation, and customer support services). In some cases, such as payment processors, the vendor or service provider may directly collect the information from you on our behalf.
- **Affiliates.** We may share personal information with and among our parent company, subsidiaries, affiliates, or their successors or assigns.
- **Clients.** We may share your personal information with our clients and companies we represent so that they may assess your suitability for employment or work as a consultant, onboard you into their systems, and credential you.
- **Marketing/Analytics/Advertising Partners.** We may share personal information with third party marketing, analytics or advertising partners, including social media platforms and networks, for commercial purposes such as sending you marketing emails.
- **Professional Advisors.** We may share information with professional advisors, such as lawyers, bankers, tax consultants, auditors, and insurers, where necessary in the course of the professional services that they render to us.
- **Government Entities.** We share information with regulatory and government entities including government, administrative, law enforcement and regulatory agencies; tax authorities; and other public agencies or authorities if we think we should in order to comply with any applicable law, regulation, legal process or other legal obligation. This includes cooperating with law enforcement when we think it is appropriate, obtaining legal remedies or limiting our damages, and to enforcing or protecting our contracts, legal rights or the rights of others, including by responding to claims asserted against us.
- **Corporate Transaction Recipients.** We may share information with potential investors, purchasers, merger partners, and their advisors in the event we: (i) sell or transfer, or are considering selling or transferring, all or a portion of our business or assets; or (ii) are considering or engaging in any reorganization, conversion, merger, sale, joint venture, assignment, transfer or disposition of all or any portion of our ownership interest, business or operations; or (iii) are soliciting or accepting investments.
- **With Your Consent or At Your Direction.** We may share information with third parties whenever you consent to or direct such sharing.
- **Other Reasons.** We may share information for other reasons we may describe to you.

In the preceding twelve (12) months, we have not sold or shared any PI.

Third parties are not allowed to use or disclose your PI other than as specified in our contract and as permitted by law.

If we seek to use your PI for a materially different purpose than we previously disclosed in this notice, we will notify you and will not use your PI for this new purpose without your explicit consent.

### **Sensitive Personal Data:**

We might need to process sensitive personal information of candidates under the California Privacy Rights Act (CPRA) if it is necessary for the recruitment or placement process and if the candidate provides explicit consent. Sensitive personal information includes data such as biometric information, and health information.

For example, we might need to process health information if a candidate is applying for a position that requires medical clearance or accommodations. In such cases, the agency would need to comply with the CPRA by obtaining the candidate's explicit consent, informing them of the purpose of collecting the sensitive information, and ensuring the information is processed securely and confidentially.

### **Your Rights:**

1. You have the right to request that we disclose certain information to you about our collection and use of your PI.
2. You have the right to be informed about the PI that we collect about you at the time that or before we collect it.
3. You have the right to request that we delete any PI about you that we have.
4. You have the right to request a correction of any inaccurate information in the PI we collect about you.
5. You have the right to stop us from sharing your PI to display advertisements to you based upon your activities, preferences, and interests.
6. If we use your sensitive PI for purposes other than the ones mentioned above, you will have the right to request that we limit the processing of your sensitive PI.
7. You will not be discriminated against or penalized for exercising your rights to your PI.
8. You have the right to request that we provide you with a copy of your personal information.
9. You have the right to direct us to limit the use or disclosure of your sensitive personal information to only the purposes specified in the CCPA.
10. Applicable law may require or permit us to decline your request.

Under the California Privacy Rights Act (CPRA) of 2024, there are certain circumstances or conditions under which an **employer can decline a candidate's request to exercise their rights. These include:**

- **Verification:** If the employer is unable to verify the identity of the individual making the request to a reasonable degree of certainty, they may decline the request.
- **Legal obligations:** If the employer is legally required to retain the personal information or is otherwise prohibited by law from deleting it, they may decline the request.

- **Exercising or defending legal claims:** If the personal information is necessary for the employer to exercise or defend legal claims, they may decline the request.  
The business needs your information to complete your transaction, provide a reasonably anticipated product or service, for certain warranty and product recall purposes, or for certain business security practices.
- **Performing services on behalf of the business:** like maintaining or service accounts, providing customer service, verifying customer information, providing storage, etc.
- **Internal purposes:** If the personal information is used for internal purposes that are compatible with the context in which the information was provided, the employer may decline the request.
- **Excessive, repetitive, or manifestly unfounded requests:** If the requests from the candidate are excessive, repetitive, or manifestly unfounded, the employer may decline them.

In all cases, the employer must provide a justification for declining the request and must inform the candidate of their right to appeal the decision.

### **How to Exercise Your Rights:**

Exercising Your Rights. To exercise any of your CCPA rights, please use our [webform](#), or call us toll free at **833-698-3362** or [email us](#).

For all requests, you must provide us with your name, email address, phone number, and mailing address. We will verify your identity by matching the information we have collected against the information you have provided. Failure to provide the foregoing information may prevent us from processing your request. Failure to provide the foregoing information may prevent us from processing your request. In order to designate an authorized agent to act on your behalf, you must provide us with a signed, written authorization. If you have requested that we correct your personal information, we may contact you to request additional information about the personal information that you believe is inaccurate, including supporting documentation.

### **Timing:**

We will acknowledge receipt of your request within 10 days of receipt of your submission. You will receive our response to your request within 45 days of your request, unless we provide you with notice that it will take more than 45 days to respond (in that case, we won't take more than 90 days to respond).

For any Opt-out of Sale/Sharing, Limit the Use of Sensitive Personal Information: we will reply to you as soon as feasibly possible, up to a maximum of 15 business days from the date they received your request.

**Appeals:**

If the business denies any of your requests, you may appeal by calling us at [phone number] or submitting your online request [online link].

**Changes:**

We will review this notice annually and update it from time to time. Any changes will be posted on this page and will become effective as of the "Last Revised" date. We encourage you to review this notice periodically to be sure you are aware of those changes.

**Social Security Number Protection Policy:**

It is our policy to protect the confidentiality of Social Security numbers ("SSNs") that we receive or collect in the course of business. We secure the confidentiality of SSNs through various means, including physical, technical, and administrative safeguards that are designed to protect against unauthorized access. It is our policy to limit access to SSNs to that which is lawful and to prohibit unlawful disclosure of SSNs.

**Changes to This Policy:**

We may change this Policy at any time. If we do so, such change will appear on this page. You may always visit this Policy to learn of any updates. Your continued access to or use of the Online Services constitutes your consent to these changes to this Policy.

**Contact Us:**

Contact us regarding this Policy or related privacy practices. If you believe we or any company associated with us has misused your Information, please contact us immediately at 833-698-3362.

**Effective date:** April 15th, 2024