

Promotion Execution Partners Workforce Privacy Notice

Effective Date: April 10, 2025

Last Updated On: April 10, 2025

This Workforce Privacy Notice (“**Notice**”) sets out how Promotion Execution Partners LLC (“**Company**”) collects, uses, discloses, and protects the personal information about our California workforce, including employees, contractors, job applicants, and job candidates who reside in California (“**Workforce**”). This Notice supplements our [Privacy Notice](#).

We are committed to protecting the privacy of our Workforce. Accordingly, we will use any Workforce personal information in accordance with this Notice. However, this Notice does not protect information you post to public areas or third-party websites, except as may be set forth herein. This Notice imposes no duties on us not imposed by state, federal, or other applicable law.

We reserve the right to modify or amend this Notice at any time to reflect changes in our personal information practices or applicable law. Should it be necessary to do so, will notify you and/or request your express consent, if required, of any material changes to this Notice by posting such changes on our Website, emailing you notice of the changes, or by other acceptable means.

Any inquiries about this Notice should be directed to us at privacy@peppromotions.com or by mail to:

Promotion Execution Partners LLC
Attn: Privacy Officer
302 W 3rd Street, Suite 900
Cincinnati, Ohio 45202

1. The Information We Collect

We may collect information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with individuals in the Workforce (“**PI**”).

PI does not include:

- Publicly available information from government records;
- Deidentified or aggregated consumer information;
- Health or medical information covered by the Health Insurance Portability and Accountability Act and the California Confidentiality of Medical Information Act; or
- PI covered by various privacy laws, including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act or the California Financial Information Privacy Act, and the Driver’s Privacy Protection Act of 1994.

We may collect PI about you through our application, recruitment, employment or engagement processes, either directly from you or (where applicable) from another person or entity such as a recruitment or professional networking website, background check provider, or from others who provide references on prospective workers. We will collect additional Workforce PI throughout the course of employment or other provision of services to us. Workforce PI may include, depending on the position:

- Identification information, such as name and date of birth.
- Contact information, such as home and business addresses, telephone numbers, and email addresses, including about your beneficiaries or emergency contacts.
- Professional or employment-related information, including:
 - Financial information, such as wages, bank account details if required for direct deposit, Social Security number, payroll records, tax identifier, and tax information.
- Business travel and expense information, such as passport information and corporate credit card usage.
- Application, recruitment, new-hire, or other engagement information, such as application forms and information included in a resume; copies of identity and immigration/work authorization documents; citizenship and residence status; background screening results and references.
- Career information, such as job title, organization charts, start and end dates, work location, appraisal and performance information, time-off records, disciplinary and grievance information, and termination details.
- Internet, electronic network, and device activity information and related identifiers, such as information about your use of our information, communication, and collaboration systems, including user IDs, passwords, IP addresses, and audit trails of system access.
- Physical security system information, such as security camera footage and security pass entry records.
- Photographs provided by or taken of you or used for work purposes.
- Sensitive information, such as demographic information and health information (e.g. disability status, leaves of absence, health and safety incidents or accidents, health insurance information, medical information related to worker's compensation claims, other medical records, and information relating to ability to perform job duties).

In particular, we may collect the following categories of PI from our Workforce:

Category	Collected
A. Identifiers , such as your full name, contact information, gender, date of birth, signature, Social Security number, driver's license or state identification numbers, and similar information for your dependents and beneficiaries.	Full name, contact information, gender, date of birth, signature, Social Security number and similar information for your dependents and beneficiaries.

<p>B. California Customer Records employment and personal information, such as your name, signature, Social Security number, physical characteristics or description, photograph, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, current employment, employment history, membership in professional organizations, licenses and certifications, bank account number, credit card number, debit card number, or any other financial, medical or health insurance information.</p>	<p>Full name, signature, Social Security number, address, telephone number, insurance policy number, education, current employment, employment history, bank account number or any other financial, medical, or health insurance information.</p>
<p>C. Protected classification characteristics under California or federal law, such as 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, reproductive health decision making, military and veteran status, or genetic information (including familial genetic information).</p>	<p>Age (40 years or older), race, national origin, citizenship, marital status, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), veteran or military status.</p>
<p>D. Commercial information, such as transaction information, purchase history, and financial details.</p>	<p>Financial details.</p>
<p>E. Biometric information, such as certain wellness metrics.</p>	<p>Participation in third-party wellness programs (optional).</p>
<p>F. Internet or other similar network activity information, including all activity on PEP information systems (such as internet browsing history, search history, intranet activity, email communications, social media postings, stored documents and emails, usernames, and passwords) and all activity on communications systems (such as phone calls, call logs, voicemails, text messages, chat logs, app use, mobile browsing and search history, mobile email communications, and other information regarding an employee's use of PEP-issued devices).</p>	<p>Browsing history, search history, all activity on PEP IT resources, pursuant to our internal policies.</p>

G. Geolocation data , such as the time and physical location related to use of an internet website, application, or device.	Time related to the use of an internet website, application, or device.
H. Sensory and surveillance data , such as COVID-19 related temperature checks and call monitoring and video surveillance.	Video surveillance, voice recordings, photographs, and video.
I. Professional or employment-related information , such as employment application information (work history, academic and professional qualifications, educational records, references), and interview notes, background check, drug testing results, work authorization, performance and disciplinary records, salary, bonus, commission, and other similar compensation data, benefit plan enrollment, participation, and claims information, leave of absence information including religious, military and family obligations, health data concerning employee and their family members.	Employment application information, current or past job history, performance evaluations, or education information.
J. Non-public education information , such as education records, degrees and vocational certifications obtained, report cards, and transcripts (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records, degrees, transcripts.
K. Inferences drawn from other personal information.	No.
L. Sensitive Information.	Social Security number; driver's license; complete account access credentials and account log-ins; precise geolocation, including access to PEP office; racial or ethnic origin; immigration status; mail, email, or text messages contents not directed to PEP; health information, including job restrictions and workplace illness and injury information.

2. How We Use Your PI

We use Workforce PI for many purposes, including:

- Workforce planning, recruitment, and hiring, including assignment planning and budgeting, job advertising, interviewing, background checking as permitted by law, and selecting and engaging individuals to join our team.

- Workforce management and administration, including onboarding, payroll processing, training administration, compensation and benefits, and performance management.
- Performance of business operations, including providing, managing, supporting, and improving information and communication systems and processes; maintaining accounts and internal directories; data administration; crisis management; processing payroll and making contractor payments; managing employee benefit plans, including enrollment and claims handling.
- Provide our Workforce with human resources management services and employee data maintenance and support services.
- Administer health wellness programs.
- Communicate with our Workforce or their emergency contacts and plan beneficiaries
- To personalize an applicant or candidate experience and to deliver content and information relevant to that purpose, including via email or text message (with your consent, where required by law).
- Comply with applicable state and federal labor, employment, tax benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws.
- Legal and regulatory compliance with policies, guidelines and contracts.
- Maintain personnel records and complying with record retention requirements.
- Prevent unauthorized access to or use of PEP property, including information systems, electronic devices, network, and data.
- To help maintain the safety, security, and integrity of our network, systems, technology assets, business, premises, customers, and other members of our Workforce.
- Ensure productivity and adherence to PEP policies.
- Conduct internal audits and investigate complaints, grievances, and suspected violations of PEP policy.
- Respond to law enforcement requests and as required by applicable law or court order.
- Exercise or defend the legal rights of PEP and its employees, affiliates, customers, contractors, and agents.
- For business structure changes, evaluations, and due diligence.
- To analyze trends, administer candidate or applicant websites, track user movement, and compile broad aggregate demographic information for reporting purposes.
- As described to you when collecting your PI or as otherwise permitted under applicable law.
- Matters relating and/or incidental to the items above.

We may use sensitive PI as follows:

- We may use information including identifiers, such as Social Security number, driver's license number, and immigration documentation, to verify eligibility for engagement, conduct background checks, process and administer compensation and benefits, provide support services, communicate with our Workforce and emergency contacts and beneficiaries, comply with applicable law, prevent compromises of PEP property, and to respond to law enforcement requests.
- We may use information relating to medical conditions and disabilities or leaves of absence to comply with (or exercise rights under) employment and other legal or contractual obligations, for workforce planning and administration, and preparing analyses and reports.
- We may use information about your precise geolocation or physical or mental health or disability status to help protect the health and safety of our workforce and workplace, to assess your fitness to work, to provide reasonable workplace accommodations and to monitor and manage absence to comply with (or exercise rights under) employment and other legal or contractual obligations, and (if necessary) to protect your or others' vital interests.
- We may use information that we may collect about your demographics and immigration status to ensure meaningful equal opportunity and diversity and inclusion monitoring and reporting, and to comply with (or exercise rights under) employment and other legal requirements.
- We may use mail, email, or text content on PEP's systems or as permitted by law to conduct investigations or exercise or defend PEP's legal rights and those of its employees, affiliates, customers, contractors, and agents.

We will not collect additional categories of PI or use the PI we collected for materially different, unrelated, or incompatible purposes without providing you notice.

3. Sharing of Personal Information

We do not and will not sell the PI, including any sensitive PI, we collect about our Workforce or share it with third parties for cross-contextual behavioral advertising.

We may disclose your PI to the following service providers solely for business purposes:

- Compensation and benefits providers,
- Payroll service providers,
- Tax and other professional advisors,
- Technology service providers,
- Corporate card issuers,
- Travel and expense management providers,
- Transport and security providers,
- HR management and administration suppliers,

- Recruiting agencies and temporary employment agencies,
- Background check providers,
- Consumer reporting agencies and/or background check providers, and
- Auditors, lawyers, and other professional services providers.

Otherwise, we may disclose Workforce PI:

- If and when required to do so by law, regulation, or court order;
- In response to a request for assistance by a law enforcement agency;
- To seek legal advice external lawyers or in connection with litigation; and
- In connection with the sale, purchase, or merger of a business or the establishment of a joint venture.

4. Your Rights and Choices

The CCPA provides California residents with specific rights regarding their PI. This section describes CCPA rights and explains how to exercise them. **You may submit a Data Subject Rights Request by following this [link](#).**

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 PI. Once we receive your request and confirm your identity, we will disclose to you:

- The specific pieces of PI collected about you;
- The categories of PI we collected about you;
- The categories of sources for the PI we collected about you;
- Our business or commercial purpose for collecting or selling that PI;
- The categories of third parties with whom we share that PI;
- If we sold, shared, or disclosed your PI for a business purpose, three separate lists disclosing:
 - Sales, identifying the PI categories that each category of recipient purchased;
 - Disclosures for a business purpose, identifying the PI categories that each category of recipient obtained; and
 - The business or commercial purpose for collecting or selling PI.

Right to Correct

You have the right to request that we correct any of your PI that we collected from you.

Right to Delete

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

- Complete the transaction for which we collected the PI, provide a service that you requested, or take actions reasonably anticipated within the context of our ongoing business or professional relationship with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Enable solely internal uses that are reasonably aligned with your expectations based on your 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 PI not subject to one of these exceptions from our records and will direct our service providers to take similar action. We commit that we will not reidentify deidentified PI.

Right to be Free From Discrimination

You have the right to be free from discrimination for exercising your privacy rights granted under the CCPA and other state data privacy laws.

Right to Opt-out of Sale or Sharing

You have the right to request that we stop selling or sharing (for cross-context behavioral advertising) your personal information (“opt-out”). However, PEP does not sell or share Workforce PI.

Right to Limit Use and Disclosure of Sensitive PI

You have the right to direct us to only use your sensitive PI (for example, your social security number, financial account information, precise geolocation data, or biometric data) for limited purposes. However, PEP does not use or disclose Workforce sensitive PI for any other purposes.

You also have the right to appeal our decision if we deny your consumer request. If we deny your request, you can send an email to privacy@peppromotions.com requesting an appeal of the denial. Within 45 days of receipt of your appeal, we will inform you of the action we took or did not take in response to your appeal. We may extend the 45-day period by an additional 15 days where reasonably necessary and inform you of the delay and the reasons for the delay. If your appeal is denied, we will provide you with an online mechanism to contact the California Attorney General where you can submit a complaint.

5. Data Security

While no method of data transmission is guaranteed against unlawful third-party interception or other misuse (for example, e-mail sent to or from our website may not be secure), we use commercially reasonable administrative, technical, and physical efforts to ensure protection of your PI from unauthorized access, disclosure, alteration, and destruction.

6. Data Retention

We will keep your PI for as long as necessary to fulfill the purposes we collected it for and in accordance with our internal document retention policy and any applicable laws. We will retain and use PI as long as you have a professional relationship with us. Thereafter, we will keep your PI for as long as is necessary (1) to protect our legal interests; and (2) to keep records required by law. We will retain PI and other information in accordance with our internal document and records retention policies. Different retention periods apply for different types of PI.