Contact Us

CA Consumer Privacy Act Policy and California Privacy Rights Enforcement Act Introduction

Document change record

Date	Version	Author	Change Details
1 February 2020	1.0	Group	Initial document
17 January 2023	1.1	Iain Struan / Ramesh Maturu	Incorporate CCRA and legal updates
10 July 2023	1.2	Iain Struan / Ramesh Maturu	Review and update
22 July 2024	1.3	Joel Lawhon	Style and layout

What are CCPA and CPRA?

The California Consumer Privacy Act ("CCPA") was enacted in 2018 and took effect on January 1, 2020. It confers new privacy rights for consumers and imposes corresponding obligations on businesses subject to it.

On November 4, 2020, California voters passed the California Privacy Rights and Enforcement Act (CPRA). The CPRA replaces and amends several parts of the existing Act, the California Consumer Privacy Act (CCPA). The new Act went into effect on January 1, 2023.

CCPA vs CPRA — What has changed?

The new data privacy act, the California Privacy Rights Act (CPRA), expands on several areas of the existing CCPA. CPRA introduces new privacy rights for California's people and adds more stringent regulations for businesses on the use of personal information. The CPRA has also established a new government agency for the enforcement of data privacy laws in California, named the California Privacy Protection Agency (CPPA). CPRA:

- Expands the definition of "businesses" covered by the privacy act and includes those "sharing" information as liable as well. Commonly controlled businesses or businesses sharing common branding are exempted unless they also share consumers' personal information.
- Introduces a new classification of personal information (PI), named sensitive personal information (SPI) that has additional use, disclosure, and opt-out requirements. This includes details like social security,

state ID, driver's license, financial account information, precise geolocation, religious or philosophical beliefs, non-public communication, genetic, biometric, and health data, etc.
- Requires organizations holding high-risk data to conduct annual cybersecurity audits, the results of which must be submitted to the CPPA.
- Expands on the CCPA's right to opt out and states that organizations must allow consumers the right to opt out of third-party sharing for advertising purposes.
- Strengthens consumers' rights by adding the right to delete or correct their personal information. If the said PI has been shared with third parties by the business, the business must notify them of the request to delete / amend as well.
- Expands on the consumers' right-to-know provisions in the CCPA.
- Introduces changes in data governance and transparency, including limitations on storage, data minimization, and contract requirements. Only data that is necessary for the purpose stated by the business must be collected, used, or disclosed. Also, data must be retained only for as long as it is necessary for the said purpose.

How does the CPRA compare with the CCPA?

The CPRA can be called a refinement or upgrade of the CCPA. The CCPA formed the basis of the data privacy landscape of California. The CPRA builds upon it to strengthen the privacy regulations in the State and bring it to par with the GDPR of the European Union.

The CPRA does not replace the CCPA per se, but surely amends it to benefit consumers and increase the compliance requirements for small and big businesses alike.

Though the CPRA went into effect on January 1, 2023, any data collected by businesses from January 1, 2022, will be subject to compliance with the CPRA. This is termed as the lookback period.

Pyramid Consulting, Inc. is committed to protecting and respecting your privacy. This privacy policy for California residents ("Policy") applies to personal information collected through our websites, applications, services, and in the course of routine offline business contact with you. It applies solely to all visitors, users, and others who reside in the State of California ("consumers," "your," or "you").

This policy has been adopted to comply with the CCPA / CPRA and any terms defined in the CCPA / CPRA have the same meaning when used in this policy. The terms "we," "us," and "our" refer to Pyramid Consulting Inc. and our operating affiliate divisions (GenSpark™ and Celsior™) (the "Organization").

How will the CPRA impact businesses?

Like any other comprehensive data privacy law, the CPRA also requires businesses to be more responsible with consumers' personal information. Businesses will need to develop stronger data protection processes and controls to be able to respond to consumer requests quickly. Businesses will also need to be agile and

adaptive enough to pivot in case of any new additions to the data privacy compliance requirements in the future.

What personal information do we collect?

For purposes of this policy, "Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with California consumers.

We may collect personal information from you in various situations, including, but not limited to, our websites, your mobile device, through email, in physical locations, through the mail, and / or over the telephone.

We collect personal information to operate, manage, and maintain our business, to provide our services, and to accomplish our business purposes and objectives. In particular, we may have collected the following categories of personal information from consumers within the last 12 months:

- Identifiers, such as names and government-issued identifiers (e.g., social security numbers).
- Personal information categories listed in the California Customer Records statute, such as contact information and financial information.
- Characteristics of protected classifications under California or federal law, such as sex.
- Biometric / Genetic information, such as fingerprints and voiceprints.
- Internet or network activity information, such as browsing history and interactions with our websites.
- Geolocation data, such as device location and Internet Protocol (IP) location.
- Audio, electronic, and similar information, such as call and video recordings.
- Professional or employment-related information, such as work history and prior employers.
- Education information, such as student records, grades, and transcripts.
- Inferences drawn from any of the personal information listed above to create a profile about, for example, an individual's preferences and characteristics.
- Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status. Some of this information is typically included in resumes or can be derived from information contained in resumes.

Personal information does not include:

- Publicly available information from government records.
- De-identified or aggregated consumer information.
- Information excluded from the CCPA's scope, such as health or medical information covered by the Health Insurance Portability and Accountability Act of 2009 (HIPAA), the California Confidentiality of Medical Information Act (CMIA), or clinical trial data; personal information covered by certain sector-specific

privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA), or the California Financial Information Privacy Act (FIPA); and the Driver's Privacy Protection Act of 1994.

The categories of sources from which we collected the personal information listed above include, but are not limited to:

- Directly from job candidates / applicants and employees. For example, when they
  - Contact the organization by phone, email, or otherwise in respect of any of its services.
  - Apply for assignments that the organization has advertised on behalf of its clients or itself.
  - Complete contract assignments at client sites, including logs of work completed and hours worked.
- Sources such as LinkedIn, corporate websites, job board websites, online CV libraries, business cards, personal recommendations, and the organization's websites.
- Service providers, including external payroll service providers, and other third parties.
- Directly from clients, contractors, or their agents. For example, from information clients provide in relation to the services for which they engage the organization.

How do we use personal information?

We may use or disclose the personal information we collect for one or more of the following business purposes:

1. **Job candidate /applicant information** — We generally use the personal information about job candidates / applicants in the following ways:
   a. Recruitment services — Because a significant area of our business is providing recruitment services, we have listed below numerous ways in which we may use and process personal information for this purpose, when appropriate and in accordance with any legal requirements. This list is not exhaustive.
      - Storing the information (and updating it when necessary) in our databases, so that we can contact job candidates / applicants in relation to recruitment.
      - Providing job candidates / applicants with our recruitment services and to facilitate the recruitment process.
      - Assessing information about job candidates / applicants to compare it against vacancies that we think might be suitable for them.
      - Sending job candidates' / applicants' information to clients, to apply for assignments or to assess their eligibility for assignments.
      - Enabling job candidates / applicants to submit their CVs, apply online for jobs, or subscribe to alerts about jobs that might be of interest to them.

- Carrying out our obligations arising from any contracts entered into between the organization and job candidates / applicants.
- Carrying out our obligations arising from any contracts entered into between the organization and third parties in relation to job candidates' / applicants' recruitment.
- Facilitating our payroll and invoicing processes.
- Verifying the details that job candidates / applicants have provided, using third party resources or by requesting additional information.
- Complying with our legal obligations in connection with the detection of crime or the collection of taxes or duties.
- Processing job candidates' / applicants' information to enable us to send them targeted, relevant marketing materials or other communications that we think are likely to be of interest to them.

2. **Marketing activities** — We may use personal information for the purposes listed below, when appropriate and in accordance with any legal requirements. This list is not exhaustive.
    a. Enabling us to develop and market other services; and
    b. Marketing our full range of recruitment services (permanent, temporary, contract, Managed Service Provider programs, etc.) to job candidates / applicants.
    c. We may use personal information to help us comply with legal or regulatory requirements for job candidates / applicants, including government reporting, investigations, legal proceedings, record-keeping, and for audit purposes.
3. **Employee information** — We use the personal information of our employees for remuneration, taxation, pension, and benefits purposes. The information requested is necessary for the performance of our obligations under their employment contracts. If employees do not provide the information requested, we will be unable to pay them their wages, provide or register them for benefits, or facilitate claims for benefits. We may also process personal information as part of performance review processes and in relation to compensation, rewards, and benefits. We also keep employee training records. We may also need to process personal information in connection with disciplinary, grievance, and dismissal processes. Additionally, we may use personal information to help us comply with legal or regulatory requirements for employees, including government reporting, investigations, legal proceedings, record-keeping, and for audit purposes.
4. **Contractor information** — We may use the personal information about our contractors to:
    a. Store (and update when necessary) their details on our databases, so that we can contact them in relation to our agreements.
    b. Offer services to them or obtain support and services from them.
    c. Perform certain legal obligations.

d. Help us to establish, exercise, or defend legal claims.

We may also use personal information to facilitate administrative functions, information technology operations, legal reasons, and corporate transactions. These functions include, but are not limited to the following:

- To manage and operate information technology and communications systems, risk management and insurance functions, budgeting, fiscal management and reporting, and strategic planning.
- To manage litigation and other legal matters and inquiries, and to meet legal and regulatory requirements.
- In connection with corporate transactions, sales, or assignments of assets; and mergers, divestitures, or other changes of control or financial status of the organization or its subsidiaries or affiliates.
- To manage licenses, permits, and authorizations applicable to our business operations.

With whom do we share personal information?

When appropriate and in accordance with legal requirements, we may share personal information in several ways and for distinct reasons, including, but not limited to:

- Individuals and organizations who hold information related to job candidates' / applicants' references or applications to collaborate with us, such as current, past, or prospective employers, educators, examining bodies, and employment and recruitment agencies.
- Tax, audit, or other authorities, when we believe in good faith that the law or regulation requires us to share this information.
- Third-party service providers who perform functions on our behalf.
- Third-party outsourced payroll providers when we have an appropriate processing agreement (or similar protections) in place.
- For job candidates / applicants:
  - Potential employers and other recruitment agencies / organizations to increase the candidates' / applicants' chances of finding employment.
  - Third-party partners, job boards, and job aggregators when we consider this will improve the chances of finding them the right job.

- Managed Service Provider (MSP) suppliers as part of our clients' MSP programs; and
- Vendor Management System (VMS) suppliers as part of work order tracking and time-capturing services for our clients.

What are your CCPA rights?

The CCPA provides certain consumers with specific rights regarding their personal information which they may exercise independently or through an authorized agent. However, it also includes several exemptions. For example, personal information about consumers who are current or former employees, job applicants, or contractors is generally exempt from, or outside the scope of, this section.

The consumers who have these rights under the CCPA may exercise them in the following manner:

1. **Right to access information**
   Consumers with these rights under the CCPA may request access to the personal information that we have collected and maintained about them (along with information regarding its use and disclosure) over the past twelve (12) months upon appropriate verification. They may make such requests two times every twelve (12) months.

2. **Right to deletion of information**
   Consumers with these rights under the CCPA may request that we delete personal information collected and maintained about them, subject to certain exceptions. Once their request is verified and we have determined that we are required to delete that information in accordance with applicable law, we will delete their personal information accordingly. Any deletion request may be denied if it is necessary for us to retain the information under one or more of the exceptions listed in the CCPA, such as complying with a legal obligation. Please note that a record of the deletion request may be kept pursuant to our legal obligations.

3. **Right to non-discrimination**
   We will not discriminate against you for exercising any of your rights under the CCPA.

How to make requests?

Consumers who have access and deletion rights under the CCPA may exercise these rights by submitting a verifiable consumer request using one of the methods described below.

- Email us at dpo@pyramidci.com.
- Make the subject line of your email "*CCPA information / deletion request*".
- Include your first and last name.
- Identify which type of request you are seeking by including one of the following sentences in your email:
  - This is a request to know categories of my personal information; or
  - This is a request to know specific pieces of my personal information; or
  - This is a request to delete my personal information.
- Include this declaration: "*I affirm that the information provided in this email is accurate, that I am the person whose full name is specified above, and that I am the owner of this email account and a California resident. I understand that the organization will contact me at the email address provided to verify I am the person making this request*".