Your Work, Your Data

A Toolkit for Exercising Worker Data Rights Under the California Consumer Privacy Act

By Kung Feng, UC Berkeley Labor Center

Nov 22, 2024

Contents

Thank you to Annette Bernhardt and Lisa Kresge at the UC Berkeley Labor Center and Minsu Longiaru at Power Switch Action for their contributions and feedback, and to the James Irvine Foundation for their support of this work.

UC BERKELEY LABOR CENTER

Part 1:

Orientation to the CCPA

What is the California Consumer Privacy Act (CCPA)?

Workers in the U.S. are virtually unprotected from companies' increasing use of digital workforce management technologies. However, a landmark change for Californians came in 2023, when workers at large businesses in the state gained basic rights around their worker data under the California Consumer Privacy Act,[1] a groundbreaking data privacy law.

Why does the CCPA matter?

The California Consumer Privacy Act, or CCPA, is an important step towards establishing worker technology rights for the 21st century workplace. Companies across the U.S. are increasingly adopting new tools including electronic monitoring and algorithmic management to monitor, profile, and control workers. Companies use data-driven technologies in ways that can have significant effects on workers' lives—like making decisions around hiring, promotion or discipline, reviewing workers' performance, and managing productivity.

Now for the first time, under the CCPA, workers have the right to know when the businesses they work for are collecting data on them and for what purpose. Workers can access their data and request to correct or delete it. They can know if companies are profiling them or buying data about them (for instance, data on their social media activity). And they can opt out of businesses selling their data.

Because of its potential value for workers and worker advocates, we explain in this toolkit the process for workers to access their data. Information gained in a data access request can reveal or substantiate unfair workplace practices and can be used to initiate challenges.

Am I covered by the CCPA?

Workers covered under the CCPA include:

- **Employees**
- **Independent contractors**
- **Job applicants**
- **Former employees**

Unless specified otherwise, our use of "worker" will include all the above categories.

[1] The CCPA was designed to protect consumers and originally excluded workers. But as of January 1, 2023, that exemption has ended, and California workers are included in its protections. The CCPA was also amended and strengthened by the 2020 California Privacy Rights Act.

Coverage by the CCPA applies to workers at large for-profit businesses in California that meet at least one of these requirements:

- Has more than $25 million in gross annual revenue, OR
- Buys, sells, or shares the personal information of 100,000 or more consumers or households, OR
- Derives 50% or more of its annual revenue from selling or sharing consumers' personal information.

Labor subcontractors and service providers (known as third parties) that control the collection of a business's worker data are bound by the same regulations as the business.

What worker data is covered by the CCPA?

Personal information

The CCPA applies to a worker's "personal information," meaning any data that can be linked to an individual worker. The following list gives examples of data that may be collected and are covered.

- Personal IDs
- Demographics
- Employment-related data
    - ◊ Evaluations
        - Customer ratings and reviews, performance metrics, peer reviews, surveys
    - ◊ Workplace activity
        - Presence and location: timeclock, at desk, in building, coworker interactions, mobile phone use, Wi-Fi access, instant messaging, bathroom usage, body movements, safety habits
    - ◊ Job activity
        - Computer activity: system login, keystrokes, screenshots, application use
        - Internet activity: email content, web searches, machine interactions such as handheld devices, industrial machines, robots, wearables, customer service interactions
        - Driving: vehicle location (GPS), acceleration, braking patterns, route, accidents, behaviors while driving and in vehicle, conversations, cell phone use
- Historical data, which could be used in a job application process
    - ◊ Credit report, criminal record, employment and salary history, education history, professional licenses and certifications, driving record, health screening, drug and alcohol test results, participation in volunteer activities, consumer activity

- Biometric data, which could be used to verify identity for time clocks or access to workspaces
    - ◊ Fingerprints, facial expressions, tone of voice, iris scans, body language
- Health and wellness data, which could be used to predict health risks and lower health care benefit costs
    - ◊ Exercise activity, sleep patterns, movement/activity level, heart rate and respiration, menstruation and pregnancy data
- Social media and digital footprint, which could be used to monitor organizing activity
    - ◊ Posts and comments on social media, blogs, online forums, and job boards
- Geolocation data, which monitors workers' location
- Audiovisual data
    - ◊ Recordings from cameras or monitoring devices

"Personal information" includes inferences made about the worker's characteristics and abilities. Inferences could include predictive scoring and ranking workers through automated decision-making systems drawing on any of the above data. For example, in an effort to decrease turnover, employers could target pay increases to workers who are predicted to be likely to quit based on their job satisfaction score, rather than to workers based on their performance or merit.

Sensitive personal information

So-called "sensitive personal information" is also covered by the CCPA and includes:

- Social Security numbers
- Union membership
- Genetic data
- Race/ethnic origin
- Health/medical data
- Biometric data
- Sexual orientation data
- Religious beliefs
- Emails not meant for the company that hired the worker

Further Information

For further information about the CCPA, or to share your experience exercising worker rights under the CCPA, contact us. We can assist you in your efforts to use your CCPA rights.

Part 2:

Summary of CCPA Rights for Workers

As of January 1, 2023, workers at large for-profit companies in California are covered by the California Consumer Privacy Act (CCPA). The law covers employees, independent contractors, job applicants, and former employees.

This is the first time that workers in the U.S. have basic rights around their worker data. These rights are an important first step in making sure that workers have the tools necessary to advocate for their rights in the 21st century data-driven workplace.

Workers have the right to know when the business they work for is collecting data on them.

Businesses must inform workers about any personal information they collect about them.

- Notice must be given **at or before** the point that the business starts collecting the data.
- Personal information means any data that can be linked to an individual worker, like personal IDs, demographics, employment-related data, biometric data, social media data, geolocation data, audio data, and inferences made about the worker's characteristics and abilities.

Specifically, businesses must give workers a notice describing:

- The categories of **worker data** they collect
- The specific **business purpose** for the data collection
- Whether the data is **sold or shared**, and how long they intend to keep the data
- What **rights** workers have under the CCPA/CPRA.

Businesses can't collect data for purposes other than those stated in the notice, or change their purpose for the data collection, without first providing additional notice to workers.

Workers have the right to get access to their worker data.

Workers have the right to request the data that the business they work for has collected about them.

- This includes data that the business has sold, shared, or disclosed.
- The business must comply with a request within 45 days, free of charge. If the business has a website, workers must be able to make a request on it.

Specifically, businesses must disclose:

- The categories of **data** it has collected about the worker in the last year
- The categories of **sources** from which that data has been collected
- The business **purpose** for the data collection, selling, or sharing
- The categories of worker data it **sold, shared, or disclosed** to third parties
- The categories of **third parties** to whom the business has sold, shared, or disclosed the worker data
- The **specific pieces of data** it has collected about the worker in the last year, in an accessible format

The business must include worker data collected by third parties (like labor subcontractors).

Workers have the right to correct and delete their data.

Workers have the right to request the business they work for to delete their data or to correct inaccurate data.

- The business must comply with the request within 45 days, and notify all third parties to do so as well.
- If the business denies a deletion or correction request, it must provide a detailed explanation to the worker.
- Note there are significant exceptions to the deletion requirement.

Workers have the right to opt out of a business's sale or sharing of their worker data.

Workers have the right to opt out of businesses selling or sharing their data to third parties such as data brokers.

- Similarly, third parties that control a businesss's worker data can't sell or share that data unless the worker has received notice and been provided the opportunity to opt out.

Workers have the right to limit businesses' use of their sensitive data.

Workers have the right to direct the business they work for to limit use of their sensitive personal data to authorized business purposes. This right to limit is only for cases when the business is using the data to profile the worker.

- Examples of sensitive worker data are Social Security numbers, union membership, genetic data, race/ethnic origin, health/medical data, biometric data, sexual orientation data, religious beliefs, and emails not meant for the business.
- Authorized business purposes are identified in the regulations, but have not yet been specified for workplace applications. Some purposes do translate, like data security, physical safety, administrative data processing, and other concepts that could potentially include workplace functions such as performance monitoring.

If a business uses or discloses workers' sensitive data for other purposes, it must first provide notice to the workers and give them the option to opt out.

General business responsibilities:

- Businesses **must limit the collection, use, and sharing of worker data** to what is "reasonably necessary" to achieve the purposes for which the data was collected or processed.
- **Third parties (labor subcontractors and service providers)** that control the collection of a business's worker data are bound by the same regulations as the business.

Worker recourse and enforcement:

- Workers can have an **authorized person or organization** make a data request on their behalf, **including unions or worker centers**.
- Businesses can't retaliate against workers for exercising their rights under this law.
- Enforcement is done by the California Privacy Protection Agency (CPPA) starting July 1, 2023, for violations occurring on that date forward. Workers do not have a private right of action for violations of the rights listed above (but they do have the right to sue the business for negligent data breaches).

Part 3:

Making a CCPA Request for Worker Data: A Step-by-Step Guide

As of January 1, 2023, workers at large companies in California have new rights around their worker data under the California Consumer Privacy Act (CCPA). These new rights include the right to access any worker data that the company they work for has collected about them. This step-by-step guide outlines the process for making a CCPA worker data request and following up on the company's response and compliance. This guide is for workers making their own requests as well as for advocates making requests on behalf of workers.

Here are the steps to make a CCPA data request:

1. Decide who will make the data request
2. Evaluate the risk of retaliation and prepare
3. Select your method of request
4. Write your data request
5. Verify your request and identity with the company
6. Track the company's responses to your request
7. Analyze the response: Did the company comply with the CCPA?

The step-by-step guide below provides details on each of the seven major steps, along with suggested actions and relevant background information. Part 4 contains a template letter that can be filled in to submit a worker data request. Please contact us for further information or questions.

Step 1: Decide who will make the data request

Action:

- **Decide whether you will make the data access request directly, or whether an "authorized agent," such as a union or other worker organization, will make the request on your behalf.**

Background:

The CCPA allows "authorized agents" to make data requests for workers with the following provisions:

- Workers can designate authorized agents, such as unions and other worker organizations and advocates, to make requests for data access, correction, or deletion on their behalf.

- The authorized agent must obtain signed permission from the worker in order to make the request on the worker's behalf.
- The company that receives the request may require the agent to provide proof that the worker gave signed permission.
- The company may also require the worker to verify their identity directly with the company, and directly confirm with the company that they provided their agent permission.
- A business cannot require the worker to provide an agent with a legal document that gives the agent a type of authorization called the "power of attorney."

Step 2: Evaluate the risk of retaliation and prepare

Note: The process of making a data request will identify you to the company. Having an authorized agent request your data on your behalf will still require disclosing your identity to the company.

Actions:

- **Consider if the company is likely to retaliate.** Take into account any possible factors which may lead to greater risk or heavier consequences, such as discrimination based on race, gender, or other identities, immigration status, or being on probation.
- **Understand the legal protections against retaliation provided by the CCPA,** as well as from labor laws that provide protection against retaliation when workers are engaging in "concerted activity" (working together to address a workplace issue).
- **Prepare accordingly.** For example, consider if there are other workers or former workers who can also make a request; educate and inoculate yourself and others around the possible ways the company might respond; and consult union representatives and legal experts.

Background:

The CCPA includes anti-retaliation protections for workers.

- Companies are specifically prohibited under the CCPA from retaliating against workers for exercising their CCPA rights. Additional legal protections may also apply depending on the circumstances. An attorney can provide you with more information on your legal rights.
- Also under federal law, union-represented workers who request their data as part of a collective action or union action/worksite campaign are legally protected from retaliation.

Step 3: Select your method of request

Actions:

- **Select a method for submitting a data request under the CCPA, from the options given by the company.**
- **If multiple workers are making a request, consider using different methods to compare results.** Companies may provide less information via one method than another. For instance, an automated response to a webform request may result in less information than if a company has to respond to a letter that details specific information requested.

Background:

A business must provide multiple methods for making a data request, such as a toll-free number, online webform, email, mail, or in person.

- A business must provide at least two methods for making a data request, one of which must be a toll-free number.
- If the business has a website, one request method must be through its website, such as through a webform.
- Other methods include email, form submitted in person, or mail.
- Information on how to submit a request can be found in the company's privacy policy, which is often linked to at the bottom of a company's webpage or shared in a company's private HR policies. See Part 5, CCPA Privacy Policy Checklist, for more information about CCPA privacy policies.

Step 4: Write your data request

Actions:

- Write your data request indicating the specific data you want to receive.
- Use the data access letter template included in Part 4 of this toolkit.
- Add specific information to the letter that is relevant to your job or workplace.

Background:

Workers can request data that was collected on or after January 1, 2022. The CCPA categorizes the data covered by the law as "personal information" and "sensitive personal information."

- "Personal information," refers to data that can be linked to an individual worker, e.g., personal IDs, demographics, employment-related data, biometric data, social media data, geolocation data, and audio data.

- "Personal information" includes inferences the company may make about the worker's characteristics and abilities based on their personal information data.
- "Sensitive personal information" includes Social Security numbers, union membership, genetic data, race/ethnic origin, health/medical data, biometric data, sexual orientation data, religious beliefs, and emails not meant for the company that hired the worker.
- More specific examples of worker data covered by the CCPA can be found in Part 1.
- A worker may request the worker data collected about them from the 12-month period immediately preceding their request.
- A worker may specifically request their worker data from before the previous 12 months as long as the data was collected on or after January 1, 2022. In this case the business must provide the data "unless doing so proves impossible or would involve disproportionate effort." The businesses would need to provide "a detailed explanation" that gives a worker a "meaningful understanding as to why." The business cannot simply state it is impossible or a disproportionate effort.

Step 5: Verify your request and identity with the company

Action:

- Verify your identity with the company and/or verify that your request is made by an authorized agent.

Background:

Businesses must verify the identity of the worker making the request in order to provide the worker the specific pieces of worker data collected about them.

- If a business has a password-protected account with the worker, it may use existing authentication procedures within the account to verify the worker.
- If feasible, businesses must match the worker's identifying information to information they already have, or use a third-party verification service. The business should avoid asking for additional information if possible. Any additional information may only be used for the purposes of verification.
- A business cannot charge the worker or their authorized agent a fee to verify their identity. If a business requires a notarized document, the business must compensate the worker for the cost of notarization.

Step 6: Track the company's responses to your request

Action:

- Document the date you made the request, and the dates and content of all the company's responses.

Background:

The CCPA has requirements for how and when the company must respond to worker data requests.

- **The company must confirm receipt of the request and provide information on how the company will process the request no later than 10 calendar days after receiving the request.**
- The company should provide information about the verification process, and when the worker can expect a response.

Step 7: Analyze the response: Did the company comply with the CCPA?

Actions:

Once the company responds by sending your data, evaluate if the company complied with the CCPA.

- Did the company respond in the required time period of 45 to 90 days?
- Check if the response is complete. Does it include all the data you expect the company has about you?
- Check if the response is accurate. Is the information provided about you correct?
- Check if the response is intelligible. Does the data come in a form that allows you to understand it?
- Be prepared that the company may not comply with all the requirements and may require follow up.
- Follow up could include sending a letter to the company, getting legal advice, and/or exploring enforcement options.

Background:

Companies must provide the requested data within 45 days, which can be extended to a maximum of 90 days. The data provided in the response must meet certain requirements, such as being in a "readily usable format." Workers may enforce their CCPA rights by filing a complaint with the California Privacy Protection Agency (CPPA).

Process and deadlines for company response:

- The company must respond by providing the requested data within 45 days. This can be extended for up to another 45 days, for a total of 90 days, but only if the business notifies the worker and explains the reasons why it needs more time.
- If the company has a password-protected account with the worker, it may use a web portal for workers to view and download a portable copy of their worker data.
- The company may deliver information through the worker's account with the business; however if the worker does not have an account, the worker can choose to have it delivered by mail or email.

Content of response:

- The CCPA has specific requirements for what information the company must provide and how it must provide it. See Part 4, the data access template letter, for the detailed requirements.
- The company must identify the categories of information, sources of information, and third parties (if applicable) in a manner that provides workers "a meaningful understanding of the categories listed."
- The data must be given in a "readily usable format" that allows the worker to transfer the data to another entity.
- The company must provide information collected by other businesses who contract with the company (third parties or service providers). The service provider or contractor must assist the company and provide the information to the company.

Unfulfilled responses:

- If the company does not fulfill the request, or fulfills it partially, the company must notify the worker and state the reason why it cannot comply with the request.
- If the request is incomplete, the company must provide instructions on how to complete the request.
- If a business cannot verify the request is from the worker whose data it collected within 45 days, it may deny the request.
- If the business cannot verify the worker's identity, then it *must not disclose* specific pieces of personal data about the worker and it must inform the worker it cannot verify identity.
- If the request is denied completely or partially, the business must still respond with categories of information even if it doesn't provide specific pieces of worker data.

Enforcement options:

- The California Privacy Protection Agency (CPPA) has enforcement powers and can investigate possible violations and impose fines.
    - ◊ Workers can file a complaint with the CPPA through an online complaint form or by printing and mailing a form.
- The California Attorney General's office can also enforce the CCPA.
- A worker does not have the right to sue the company under the CCPA, except in cases of data breaches.

Part 4:

CCPA Template Data Access Letter

(Created by Power Switch Action)

Submitted via [state method of submission here]

[Data Requestor's Name]
[Data Requestor Address 1]
[Data Requestor Address 2]
[Data Requestor Email]

[Date]

Re: California Consumer Privacy Act Data Request for Personal Information

Dear Privacy Compliance Officer:

My name is [Data Requestor Name] ("Consumer"). I reside in California and am exercising my "right to know" under the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("CPRA," collectively, "CCPA") to request that [Official Name of Company X], including its parents, divisions, subdivisions, subsidiaries, successors, and assigns (collectively, "Company X"), disclose personal information that **it has collected, sold, or shared about me, or that it has disclosed for a business purpose, in the preceding 12 months** as set forth in California Civil Code sections 1798.110 and 1798.115, as well as **personal information that [Company X] has collected on or after January 1, 2022,** as set forth in California Code of Regulations, title 11, section 7024(h).

I am making this data request in my capacity as a [current or former] [employee, independent contractor, job title(s), or job applicant] of [Company X].

Specifically, I am requesting that [Company X] disclose to me:

1. **The categories of personal information [Company X] has collected about me,** as set forth in California Civil Code sections 1798.110(a)(1) and 1798.115(a)(1);

2. **The categories of personal information that [Company X]** sold or shared about me**,** and the categories of third parties to whom the personal information was sold or shared, by category or categories of personal information for each category of third parties to whom the personal information was sold or shared, as set forth in California Civil Code section 1798.115(a)(2);

3. **The categories of personal information that [Company X] disclosed about me for a business purpose, and the categories of persons to whom it was disclosed for a business purpose,** as set forth in California Civil Code section 1798.115(a)(3);

4. **The categories of sources from which the personal information is collected** as set forth in California Civil Code section 1798.110(a)(2);

5. **The business or commercial purpose for collecting, selling, or sharing the personal information** as set forth in California Civil Code section 1798.110(a)(3);

6. **The categories of third parties to whom [Company X] discloses personal information** as set forth in California Civil Code section 1798.110(a)(4);

7. **The specific pieces of personal information [Company X] has collected about me, directly or indirectly, including through or by a service provider or contractor** as set forth in California Civil Code sections 1798.110(a)(5) and 1798.130(a)(3)(A). As used in this Request, "personal information" means "personal information" as defined in California Civil Code section 1798.140(v)(1). It includes, **but is not limited to,** the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with me or my household:
    a. Identifiers as set forth in California Civil Code section 1798.140(v)(1)(A);
    b. Any personal information described in subdivision (e) of California Civil Code section 1798.80 as set forth in California Civil Code section 1798.140(v)(1)(B);
    c. Characteristics of protected classifications under California or federal law as set forth in California Civil Code section 1798.140(v)(1)(C);
    d. Commercial information as set forth in California Civil Code section 1798.140(v)(1)(D);
    e. Biometric information as set forth in California Civil Code section 1798.140(v)(1)(E);
    f. Internet or other electronic network activity information as set forth in California Civil Code section 1798.140(v)(1)(F);
    g. Geolocation data as set forth in California Civil Code section 1798.140(v)(1)(G);
    h. Audio, electronic, visual, thermal, olfactory, or similar information as set forth in California Civil Code section 1798.140(v)(1)(H);
    i. Professional or employment-related information as set forth in California Civil Code section 1798.140(v)(1)(I);
    j. Education information, as set forth in California Civil Code section 1798.140(v)(1)(J);
    k. Inferences drawn from any information identified California Civil Code section 1798.140(v) to create a profile about me reflecting my preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes, as set forth in California Civil Code section 1798.140(v)(1)(K);
    l. Sensitive personal information, as set forth in California Civil Code sections 1798.140(v)(1)(L) and 1798.140(ae); **and**
    m. The information listed in **Attachment A** of this document. [Optional]

My email address is [Data Requestor email here], my mailing address is [Data Requestor mailing address here], and my phone number is [phone number].

According to California Code of Regulations, title 11, section 7021(a), **[Company X]** must, no later than 10 business days after receiving this request, confirm receipt of this request and provide information on how **[Company X]** will process the request. Further, this information must be provided to me **free of charge and, within 45 days of [Company X's] receipt** of this request (subject to a one-time extension in accordance with the section's requirements), must be delivered to me in a readily useable format that allows me to transmit this information from one entity to another without hindrance. (California Civil Code section 1798.130(a)(2)(A).)

Pursuant to California Civil Code section 1798.130(a)(2)(A), I request that this information be made available to me in writing and delivered through my current account with **[Company X]** or, if at the time of the delivery, I do not maintain an account, electronically.

Please be advised that **[Company X]** is strictly prohibited from discriminating and retaliating against me because I exercised my rights under the CCPA. (California Civil Code section 1798.125.)

According to the California Consumer Privacy Act Regulations (Cal. Code Regs., tit. 11, § 7020(e)), "If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either: (1) Treat the request as if it had been submitted in accordance with the business's designated manner, or (2) Provide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request, if applicable." If you choose the second option, please provide the required directions.

If you need any more information from me, please let me know as soon as possible. If you cannot comply with my request—either in whole or in part—please state the reason why you cannot comply. If my request is incomplete, please provide me with specific instructions on how to complete my request.

Sincerely,

[Requestor Name]

Enclosure: **Attachment A -** ***Consider reading Company X's data privacy policy for information on the data the company collects, and specifically listing any items which you are particularly interested in requesting, in a separate attachment. If you like, for each item, you can also include a reference to the section of the privacy policy in which the data appears.***

Part 5:

CCPA Privacy Policy Checklist

As of the beginning of 2023, workers at large companies in California have new rights around their data under the California Consumer Privacy Act (CCPA). Under the CCPA, businesses must provide workers and consumers information about their data rights and businesses' data practices in their online privacy policies.

This checklist outlines the requirements for CCPA privacy policies and includes information that may be useful for a data access request.

Important to know: The CCPA was initially written for consumers and later covered workers. Therefore, businesses' privacy policies may only refer to "consumers" and "personal information"—but those terms now cover workers and worker data.

The CCPA requires that businesses' privacy policies:

- Provide a "comprehensive description" of a business's online and offline information practices
- Inform workers and consumers of their rights regarding their "personal information"
- Provide information necessary to exercise those rights.

This information must be made available in the business's online privacy policy, in any California-specific description of consumer privacy rights, or on its website.

The following checklist outlines the specific requirements of CCPA privacy policies, including their content and when, where, and how they should be posted.

Please contact us for further information, questions, or for support reviewing your company's privacy policy.

A: Required Content

☐ Description of the worker data that the business collects about workers

The notice must describe the following in a manner that provides a meaningful understanding of the types of worker data that the business collects.

- ☐ Types of worker data ***collected***
  - ☐ Categories of worker data collected in the preceding 12 months
  - ☐ Categories of sources from which the worker data is collected
  - ☐ Specific business or commercial purpose for collecting worker data

- [ ] Types of worker data ***sold or shared***
    - [ ] Categories of worker data sold or shared in the preceding 12 months
    - [ ] Categories of third parties to whom information is sold or shared for each category of worker data collected
    - [ ] Specific business or commercial purpose for selling or sharing worker data
    - [ ] Disclose if no information was sold or shared in last 12 months
- [ ] Types of worker data ***disclosed*** for a business purpose
    - [ ] Categories of worker data disclosed in the preceding 12 months
    - [ ] Categories of third parties to whom information was disclosed for each category of worker data collected
    - [ ] Specific business or commercial purpose for disclosing worker data.
    - [ ] Disclose if no information was disclosed in last 12 months

The business must also

- [ ] Describe the worker data **sold or shared** and the worker data **disclosed** in two separate lists
- [ ] Prominently disclose in the privacy policies if the business has not sold or shared or disclosed the information in the preceding 12 months
- [ ] State whether the business discloses **sensitive worker data** for purposes other than those allowed by the CCPA

☐ Explanation of workers' rights under the CCPA

The notice must include explanations regarding workers':

- [ ] **Right to know** what worker data the business has collected, including all categories of worker data listed in the previous section
- [ ] **Right to access** (request a copy of) the specific pieces of worker data
- [ ] **Right to delete** worker data that the business has collected, subject to certain exceptions
- [ ] **Right to correct** inaccurate worker data that a business maintains
- [ ] **Right to opt out of sale or sharing** of worker data
- [ ] **Right not to receive discriminatory treatment or be retaliated against** for exercising CCPA rights
- [ ] **Right to limit the collection of the workers' sensitive worker data** for purposes other than those allowed by the CCPA

- [ ] **Explanation of how to exercise rights and what workers can expect from the process**
  - [ ] Instructions on how to submit a request, including web portal if offered
  - [ ] Notice of right to opt out of the sale or sharing of worker data
  - [ ] Notice of right to limit the use or disclosure of sensitive worker data
  - [ ] Explanation of the identify verification process used by the business to verify a worker's request to know / delete / correct, including any information a worker must provide
  - [ ] Explanation of how the business processes a request to opt-out of the sale or sharing of worker data and how to submit a request
  - [ ] Instructions on how an authorized agent can make a CCPA request on behalf of a worker
  - [ ] A contact for questions or concerns "reflecting the manner in which the business primarily interacts" with the worker

B. Requirements about when/where/how to post notices

- [ ] **Date**
  - [ ] Date privacy policy was last updated
  - [ ] Policy must be updated at least once every 12 months
- [ ] **Placement of Privacy Policy**
  - [ ] Conspicuous link using the word "privacy" on homepage, or mobile app download or landing page
  - [ ] Mobile app may also provide link in settings menu
  - [ ] A business that does not have a website must make the privacy policy "conspicuously available" to workers
- [ ] **Form of Privacy Policy**
  - [ ] "Easy to read and understandable" to workers. Uses "plain straightforward language and avoid[s] technical or legal jargon."
  - [ ] Available in languages used by the business in its usual communication with workers
  - [ ] Format that can be printed in a document
  - [ ] "Reasonably accessible" to people with disabilities