osano

# GET READY FOR EMPLOYEE DSARS IN CALIFORNIA

## “This subdivision shall become inoperative on January 1, 2023.”

There are a lot of changes that the California Privacy Rights Act (CPRA) made to the California Consumer Protection Act (CCPA), but those nine words might be the most impactful. Previously, businesses did not have to fulfill employee data subject access rights (DSARs) requests, unlike consumer DSAR requests. These nine words mean that when an employee asks to access, delete, update, or make any other DSAR request in relation to their data, businesses must comply.

And unlike consumer DSAR requests, employee requests are categorically riskier and more complex.

To help businesses become prepared for employee DSARs in California, review this infographic to find out what you need to know and what you need to do to stay compliant.

## WHAT TO KNOW

### Are you subject to the CCPA/CPRA?

If so, you'll need to comply with employee DSAR requests. The CCPA/CPRA applies to any for-profit business that does business within the state of California and that:

- Has a gross revenue of at least $25 million, or
- Collects the personal information of at least 100,000 California Residents, or
- Derives at least 50% of its revenue from the sale or sharing of the personal information of California residents.

### Understand employee rights and your responsibilities

Under the CCPA/CPRA, employees have the right to:

- Know about the collection of their personal information and to whom it is shared with or sold to
- Access the personal information you've collected
- Correct their personal information when they believe it is inaccurate
- Request the deletion of the personal information you've collected from them
- Restrict the use of their sensitive personal information, such as their social security number, sexual orientation, and other types of personal information the CCPA/CPRA defines as “sensitive”
- Not be retaliated against for exercising their rights
- Opt out of the sale or share of their personal information to third parties

### Understand the risk

Employee personal information and DSAR requests often carry more risk compared to those of regular consumers. For one, you'll likely collect more sensitive personal information from an employee, which is associated with higher penalties for violations. Furthermore, employees are more likely to make DSAR requests when they are dissatisfied. They may, for instance, make vexatious requests or go “fishing” for grounds to sue in response to a negative career event. Finally, anything that can be construed as retaliation for an employee exercising their rights may put you at risk of noncompliance or a lawsuit.

### Know when you are exempt from fulfilling DSAR requests

The law acknowledges that not all DSAR requests will be legitimate. You aren't obligated to fulfill a request if it is “manifestly unfounded or excessive.” If an employee makes repeated DSAR requests that repeat the same action and/or appear to be purely vexatious in nature, then you can notify the employee that you will not act. However, it's up to you to demonstrate why the request is manifestly unfounded or excessive.

## USE OSANO TO STREAMLINE YOUR DSAR PROCESS

Becoming compliant with the CCPA/CPRA doesn't have to be overwhelming. The Osano Privacy Management Platform enables businesses to manage employee DSARs in a safe and secure way that minimizes disruption to your daily operations.

With Osano's Subject Rights Management and Data Discovery products, you can:

- Manage the end-to-end DSAR process without relying on emails and spreadsheets
- Discover relevant data throughout your organization and coordinate with data store owners
- Scale your compliance efforts as you grow your organization and privacy program

## WHAT TO DO

### Respond within 45 days

By default, businesses must respond to a DSAR request within 45 days, with an optional 45-day extension when processing requests related to knowing, deleting, or correcting data. Note that opt-out requests must be processed within 15 days at most.

### Verify the requestor's identity

If the requestor asks to know, delete, or correct their data, then you must verify that the requestor is indeed the person associated with the data.

### Collect only the data you need

You'll already be collecting a significant amount of employee personal information in the course of your normal business activities. There's no need or benefit to collecting any additional data beyond that—all you'll be doing is increasing your burden and your risk when acting upon employee DSAR requests.

### Keep employee data only for as long as is necessary

By the same token, there's no need to hang onto all employee data forever. Retaining data beyond its usefulness will create a bigger workload for you down the line when you have to fulfill DSAR requests related to that data.

### Conduct a data inventory/RoPA

A data inventory or record of processing activity (RoPA) isn't explicitly required by the CCPA/CPRA, but it's functionally essential for DSAR compliance. Keeping a record of where different types of data lives, who handles it, where it's sent to, what category it falls under, and so on is critical for any data privacy compliance activities.

### Develop an employee privacy policy

Under the CCPA/CPRA, employees have the right to be informed about what personal information you collect from them and what you do with that information, making an employee privacy policy an essential document for compliance. Not only will developing this policy encourage you to think about your organization's privacy program, but it also goes a long way toward building up trust with your employees.

### Avoid email and spreadsheets

Using emails and spreadsheets to manually communicate with data subjects, track what's been done with what data, coordinate with data store owners across your organization, and tackle all of the individual tasks in your DSAR workflow is prohibitively error-prone and time-consuming. In the long-term, it's simply unsustainable as your DSAR volume grows.

### Centralize your workflow

Rather than use emails and spreadsheets to manage the DSAR workflow, identify a purpose-built DSAR solution, ideally within an overall compliance platform. Since carefully managing data is so central to DSAR compliance, centralizing your entire DSAR workflow in one tool will help you cut down on data bloat, identify which tasks need to be completed and when, and streamline your process.

### Make your data discoverable

Whether you manage the DSAR workflow manually or through a purpose-built solution, automated data discovery is a must. Even the smallest organizations will have too many data stores and too many fields to manually search through for every DSAR request; you'll want to identify a way to search through your data stores all at once. Many data privacy compliance platforms feature both a workflow management tool for DSAR requests as well as data discovery capabilities.

SCHEDULE A FREE DEMO

osano

@osano
linkedin.com/company/osano
http://facebook.com/osanoatx

osano.com

### About Osano

Osano is a complete data privacy platform trusted by thousands of organizations around the world. Its platform simplifies compliance for complex data privacy laws such as GDPR, CCPS, LGPD, and more. Features include consent management, subject rights management, data discovery, and vendor risk monitoring. Osano is the most popular cookie compliance solution in the world, used on over 900,000 website to capture consent for more than 2.5 billion monthly visitors.