

QUICK GUIDE

# CPRA Do Not Sell or Share

Each question below corresponds to a requirement outlined in the CPRA Final Regulations. Check the boxes to track your answers and explore applicable guidance on the right hand side.



Nothing contained in this guide constitutes legal advice. If you have any questions regarding your legal rights and obligations, consult with your attorney.

01

**Does your business sell or share consumers' personal information to a third party for valuable consideration or for targeted advertising?**

☐ Check if this applies to you

02

**Are you collecting data on your business's website with the intent to sell or share?**

☐ Check if this applies to you

03

**Are you allowing a third party to collect data for advertising purposes?**

☐ Check if this applies to you

If you answered **YES** to **ANY** of the questions above, your business must allow consumers visiting your website to opt out via a link in your Privacy Policy **AND** via privacy preference signals like Global Privacy Control (GPC).

Continue below



If you answered **NO** to all of the questions above—no need to continue,

**CPRA Do Not Sell or Share does not apply to you!**

No need to continue



04

**Are you selling or sharing consumer data via offline or backend processes?**

*For example, uploading user lists to a targeted advertising tool, sending user data to an advertising API, or using a customer data platform to distribute data to partners.*

☐ Check if this applies to you

## Request additional information

To effectively process a consumer's opt-out request, you may need to collect additional information about their identity—for example, their log-in credentials or email address.

05

**Can visitors create an account and/or log-in on your website?**

☐ Check if this applies to you

## Ensure future opt-out and resolve potential conflicts with other privacy settings

You may need to:

- Store a logged-in user's opt-out preference to ensure it's honored on future site visits
- Resolve potential conflicts between the user's opt-out signal and their privacy settings specific to your business

*For example, while CPRA requires you to honor opt-out signals and immediately process opt-out requests, you can ask users if they're willing to re-consent and/or give you permission to ignore their opt-out preference signal.*

06

**Does your company use or disclose consumers' Sensitive Personal Information (SPI)?**

*Examples of SPI include Social Security Number, Driver's License number, financial account information, precise geolocation data, ethnic origin, or health information.*

☐ Check if this applies to you

## Review Section §7027 and consider implementing an SPI opt-out process

Carefully review Section §7027 of the Final Regulations and consult with legal counsel to understand how the regulations apply to you.

You may need to set up an additional opt-out process allowing users to request that you limit the use and disclosure of their SPI.

07

**Do you offer financial incentives in exchange for collecting consumers' personal information?**

*For example—a loyalty or discount program, or offering a higher level of service for consumers who allow collection.*

☐ Check if this applies to you

## Provide notice and handle opt-out conflicts

Regardless of a consumer's opt-out preference, your business must provide a "Notice of Financial Incentive."

If a consumer's opt-out preference conflicts with their participation in the financial incentive program, notify them that honoring their opt-out signal would withdraw them from the program and confirm their intent to withdraw.

08

**Did you answer **NO** to questions #2-7?**

☐ Check if this applies to you

## Consider frictionless opt-outs

If your business follows an opt-out process that minimizes user friction, as outlined by the Final Regulations, you don't need to include opt out links in your business's website footer.

09

**Implementation considerations for everyone**

## Do Not Sell or Share best practices

- Work with legal counsel to update your privacy policy to include all CCPA/CPRA mandated disclosures regarding sale and sharing of information, honoring of GPC signal, etc.
- Look very critically at any third party trackers you're using. If an exchange of information with the third party could constitute a service provider relationship, make sure you have a service provider agreement in place.

# Simplify Do Not Sell or Share with Transcend

Take the stress out of CPRA Do Not Sell or Share requirements and support compliance with state laws in Virginia, Colorado, and Utah. Automatically identify advertising technologies and comply with privacy signals like GPC to honor opt-out requests correctly.

With Transcend Consent, you can catalog your advertising tech to understand what technologies are processing personal information. Using this data inventory, you can govern your data flows—both on the browser side (via trackers on your website) and your backend (sending data to a CDP like Segment).