BigID

A GUIDE TO CPRA

Get the guide to get ahead of the California Privacy Rights Act (CPRA), the next evolution of California privacy regulations.

Learn what's new, what's changed, and how to get ready for CPRA.

HOW TO PREPARE FOR CPRA COMPLIANCE

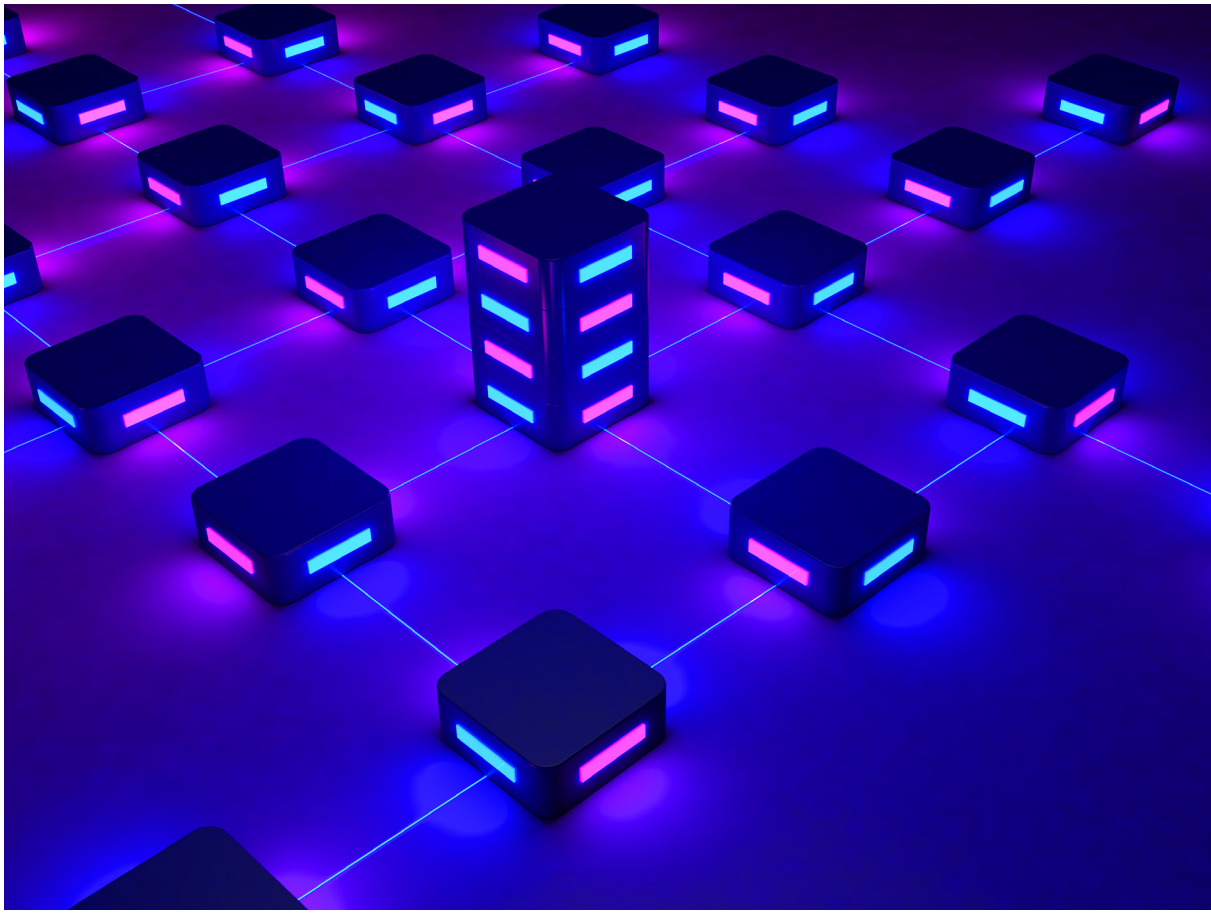
The California Privacy Rights Act (CPRA), is the next evolution of California privacy regulations, aimed at strengthening and expanding the California Consumer Privacy Act (CCPA).

From steeper data disclosure requirements to stronger enforcement, CPRA builds upon CCPA's core protections for consumers, gives individuals more control over their data, and creates stricter compliance requirements for organizations.

This guide will take you through what's new and what's changed, from new definitions of Sensitive Personal Information (SPI) to expanded data breach liabilities — and how to get your organization ready for CPRA compliance.

IN THIS CPRA GUIDE, YOU'LL LEARN:

- NEW PROVISIONS UNDER CPRA
- HOW THE CPRA EXPANDS CCPA
- HOW TO PREPARE FOR THE CPRA
- WHERE TO START WITH CPRA COMPLIANCE



NEW: DEDICATED ENFORCEMENT AGENCY

HOW IT STRENGTHENS CCPA

Under CCPA, enforcement for violations goes through the California Attorney General's office. CPRA establishes the California Privacy Protection Agency, the first agency in the U.S. with rulemaking authority that is exclusively devoted to privacy enforcement.

HOW TO PREPARE

Be ready to quickly respond to regulatory requirements and fulfill data requests at scale with advanced reporting and analysis — including native reporting, trends, and executive reports.

NEW: SENSITIVE PERSONAL INFORMATION (SPI) DEFINITION

HOW IT STRENGTHENS CCPA

"Sensitive personal information" (SPI) is a new term under CPRA that goes beyond CCPA's personal information (PI) definition. Expanding the definition will bring more information under compliance. SPI includes:

- SSNS
- DRIVERS LICENSE AND STATE ID NUMBERS
- PASSPORT INFO
- PRECISE GEOLOCATION
- USER CREDENTIALS
- FINANCIAL AND HEALTH INFORMATION
- "SEX LIFE" OR SEXUAL ORIENTATION DATA
- BIOMETRIC AND GENETIC DATA
- RACIAL OR ETHNIC ORIGIN INFO
- RELIGIOUS OR PHILOSOPHICAL BELIEFS
- UNION MEMBERSHIP
- CONTENTS OF MAIL, EMAIL, AND SMS MESSAGES

HOW TO PREPARE

Automatically discover, identify, and classify all SPI wherever it lives — on-prem, in the cloud, and hybrid — across all data sources, at petabyte scale.

NEW:
THE RIGHT TO CORRECTION

HOW IT STRENGTHENS CCPA

The game-changing stipulation says that companies must offer consumers the ability to update and correct inaccurate information a company may have about them.

HOW TO PREPARE

Discover and inventory all sensitive and personal data belonging to an identity — direct and inferred — for a full picture of what consumer data your organization is collecting.

NEW:
THE RIGHT TO LIMIT THE USE AND DISCLOSURE OF SPI

HOW IT STRENGTHENS CCPA

This allows consumers to limit the collection and processing of their SPI to only those purposes "necessary" for providing the goods or services they've requested.

HOW TO PREPARE

Add context to data with advanced classification and correlation. Uncover relationships, infer new attributes, and view data according to its purpose of use.

EXPANDED: THE RIGHT TO KNOW

HOW IT STRENGTHENS CCPA

The CPRA broadens the scope of CCPA's "right to know" to include personal information that is sold or shared — not just collected. Businesses must also now disclose upfront what categories of information they will collect or share with a third party.

HOW TO PREPARE

Inventory SPI, document data flows, and automate "right to know" fulfillment processes for a stronger privacy management program.

EXPANDED: THE RIGHT TO DELETE

HOW IT STRENGTHENS CCPA

CPRA expands CCPA's "right to delete" to require that businesses notify contractors, service providers, and all third parties of a consumer deletion request — and that those third parties cooperate in deleting the information, and continue to pass the request downstream.

HOW TO PREPARE

Determine what data should be deleted, where it's located, and automatically ensure ongoing deletion validation.

EXPANDED: DO NOT SELL OR SHARE

HOW IT STRENGTHENS CCPA

The “do not sell” provision that allowed consumers to opt out of the sale of their personal information under CCPA now includes an expanded right to opt out of the sharing of their information — not just its sale — for behavioral advertising purposes.

HOW TO PREPARE

Track and document preference management, consent, and all third-party data sharing.

EXPANDED: DATA MINIMIZATION AND DATA RETENTION

HOW IT STRENGTHENS CCPA

Under CPRA, businesses have to disclose how long they keep data and ensure that the timeline is only as long as is “reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed.”

HOW TO PREPARE

Define and enforce data retention rules with automated workflows. Uncover duplicate, derivative, and similar data for privacy-compliant governance and effective reporting.

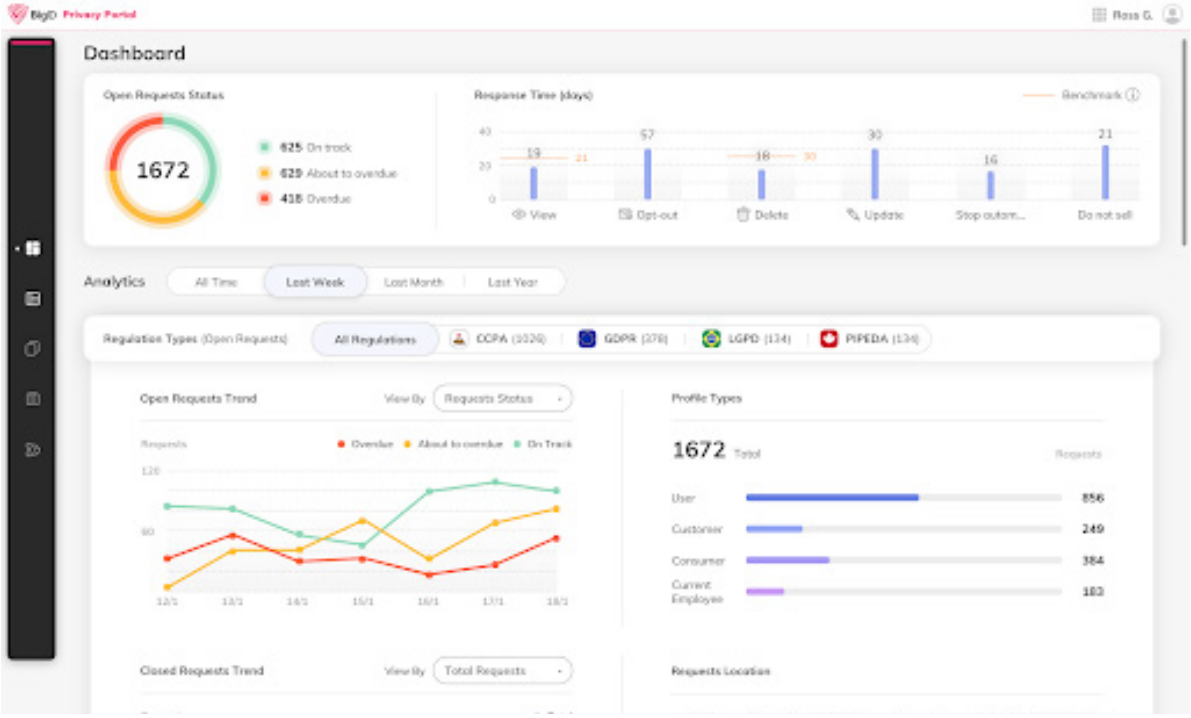
EXPANDED: DATA BREACH LIABILITY

HOW IT STRENGTHENS CCPA

The CPRA amends CCPA's data breach liability provision to include breaches resulting in the compromise of a consumer's email address in combination with other data, like a password or security question. This is in line with a growing number of states, such as New York's SHIELD Act.

HOW TO PREPARE

Discover and correlate personal information — like an email address with a password — to better protect it from potential breaches. Identify potentially impacted users from known data breaches for proactive incident response.



HOW BIGID CAN HELP YOUR COMPANY GET AHEAD OF CPRA

To address evolving privacy regulations like the CPRA, start with a privacy-centric approach to your data.

BigID's privacy-centric data discovery and catalog is purpose-built to address evolving data privacy and protection regulations like CPRA — along with evolving definitions of personal and sensitive data. Traditional approaches to data discovery do not consistently identify the data in scope under CPRA, especially with the newly defined SPI.

BigID gives you a unified inventory of all your data in one place, wherever it lives — in a single pane of glass.

The consolidated view into your consumer, customer, employee, sensitive, vulnerable, and at-risk data makes it easier for your organization to extend your data privacy policies to address the new and updated CPRA guidelines, including the ability to:

1. Report on your data — quickly and accurately
2. Discover SPI and understand whose data it is — within the context of PI and SPI (including geolocation)
3. Easily identify data for correction
4. Classify data according to its purpose of use — plus other attributes and contexts
5. Automate “right to know” fulfillment
6. Flag data that should be deleted, and automate deletion workflows
7. Ensure you’re sharing the right data with third parties
8. Minimize duplicate data and apply retention rules for SPI based on a disclosed purpose
9. Apply controls for breach risk reduction and enable proactive incident response

Learn more about how BigID can help you stay ahead of the evolving privacy regulation landscape and achieve CPRA compliance — click here to get a demo and see BigID in action.