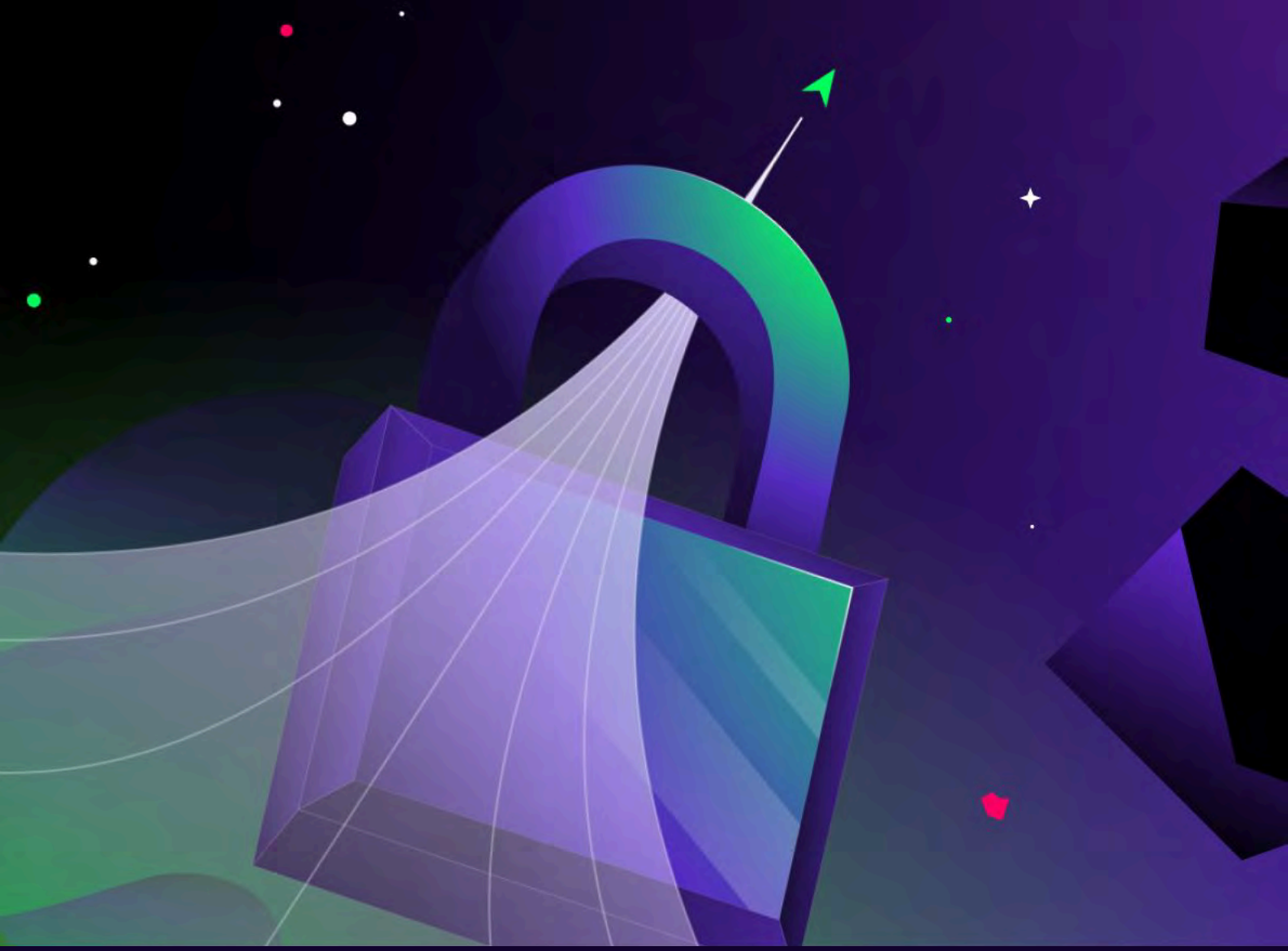
CYERA

Protecting PII in California and Beyond

How Cyera Supports Compliance with the CCPA and CPRA

Table of Contents



Introduction

About the CCPA and the CPRA

The California Consumer Privacy Act (CCPA), enacted in 2018 and effective January 2020, was the first comprehensive U.S. state law granting residents greater control over their personal data. It provides rights to know what data is collected, request deletion, opt out of data sales, and access equal service without discrimination.

In 2020, voters approved the California Privacy Rights Act (CPRA), which took effect in 2023, expanding and strengthening the CCPA. The CPRA created the California Privacy Protection Agency, introduced new rights such as correction of inaccurate data, and applied stricter rules to "sensitive personal information."

Both laws require businesses to implement robust data protection practices, update privacy notices, and ensure transparency in data usage. Their importance lies in establishing the most rigorous U.S. privacy standards, pushing companies to enhance data security, and influencing broader national and international privacy frameworks by prioritizing consumer rights and accountability.

About Cyera

Cyera is a unified, AI-native data security platform that empowers businesses to manage sensitive data across highly permissive and widely distributed environments with precision and efficiency.

The platform's non-invasive, automated data discovery provides a comprehensive view of sensitive data across structured and unstructured sources. This capability enables organizations to address critical challenges like data proliferation. Powered by AI-driven classification, Cyera goes beyond traditional methods by understanding context, intent, and nuance. This deep insight helps uncover ghost data, reveal data risks, reduce false positives, and mitigate threats like data breaches and ransomware — areas where conventional data loss prevention and data governance tools fall short.

By combining advanced technology with ease of use, Cyera empowers organizations to confidently secure personal data, support CCPA and CPRA compliance, and safely enable AI use cases.

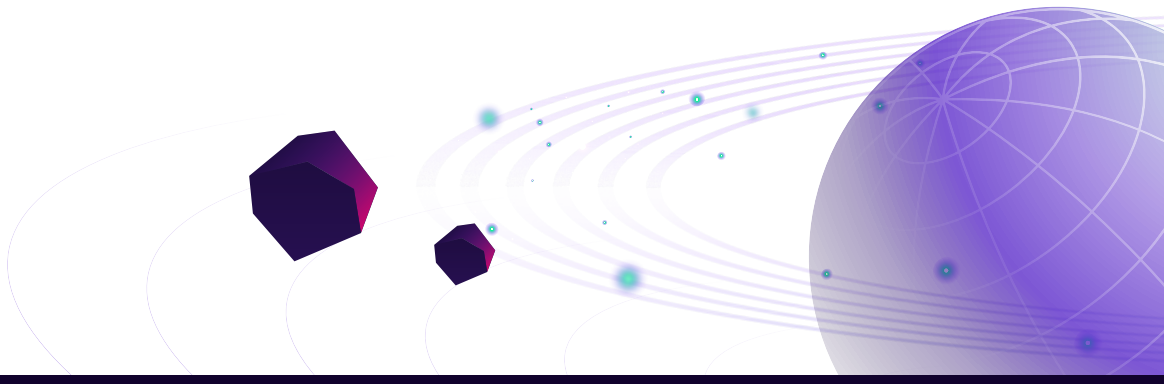
Duties of Businesses that Collect Personal Information

The CCPA and CPRA together impose several important obligations on businesses that control the collection of consumers' personal information. Together, these obligations establish essential guardrails for industry and form the basis for consumers' reasonable expectations when it comes to the privacy of their personal information. These obligations include:

- **Transparency:** Business that control the collection of consumers' personal information must inform them of:
  - The categories of personal information that will be collected and used, including any categories of sensitive personal information;
  - The purpose(s) for which personal information is collected and used;
  - Whether the personal information collected will be shared or sold to third parties; and
  - The length of time the business intends to retain each category of personal information.
- **Purpose Limitation:** Businesses that control the collection of consumers' personal information must not use that information for purposes that are incompatible with the disclosed purpose for its collection.

  A purpose is incompatible with the disclosed purpose if it is not reasonably necessary or proportionate to fulfilling the disclosed purpose, and if a reasonable consumer would not expect their information to be used for the alternative purpose.
- **Minimization:** Businesses that control the collection of consumers' personal information must not collect or use any additional categories of personal information than those necessary to fulfill the purpose for which it is collected.

  They must also not use or share more personal information than necessary, or retain it longer than necessary, to fulfill the purpose of its collection.
- **Duty to Protect Personal Information:** Businesses that control the collection of consumers' personal information must implement reasonable security procedures and practices in order to protect it from unauthorized or illegal access, use, disclosure, modification, or destruction.
- **Duty to Supervise Third Parties:** Businesses that sell or share consumers' personal information to third parties for business purposes must enter into agreements with those third parties to ensure that the latter also honor the obligations of purpose limitation, minimization, and protection of personal information.



Cyera supports minimization and data retention requirements by discovering dormant personal data and orphaned data stores. It allows you to review datastore and file age and pinpoint retention issues. And it can validate secure deletion of files and datastores to demonstrate compliance with organizational and regulatory data retention policies.

Cyera's data security platform helps you protect consumers' personal data. Cyera's DSPM discovers and classifies personal data across cloud and on-prem resources. It can identify unencrypted personal data at rest or in motion, and apply policies to obfuscate unencrypted data and alert data owners to take remedial actions.

Cyera's AI Security Posture Management identifies AI apps and tools, including public, embedded, and homegrown AI, in use in your environment. And Cyera's AI Runtime Protection can redact or block sensitive categories of data in prompts, logs, and AI outputs.

Cyera integrates with identity providers like Okta to create a catalog of identities with access to your data estate, including internal and external users. Cyera can identify stale or ghost identities that should no longer have access, and can see which entities have disabled multifactor authentication.

Cyera also offers a number of professional services - including its Data Risk Assessment, Breach Readiness, and AI Risk Assessment, that can help you evaluate and improve the effectiveness of the technical and organizational measures you have implemented for data security.

Cyera helps you supervise third party processors by giving you visibility into which identities are accessing your data and what actions they have taken.

Finally, Cyera Privacy will soon include consent management capabilities, allowing your organization to manage user consent for cookies, tracking technologies, mobile software development kits (SDKs), and other processing activities.

Consumers' Data Privacy Rights

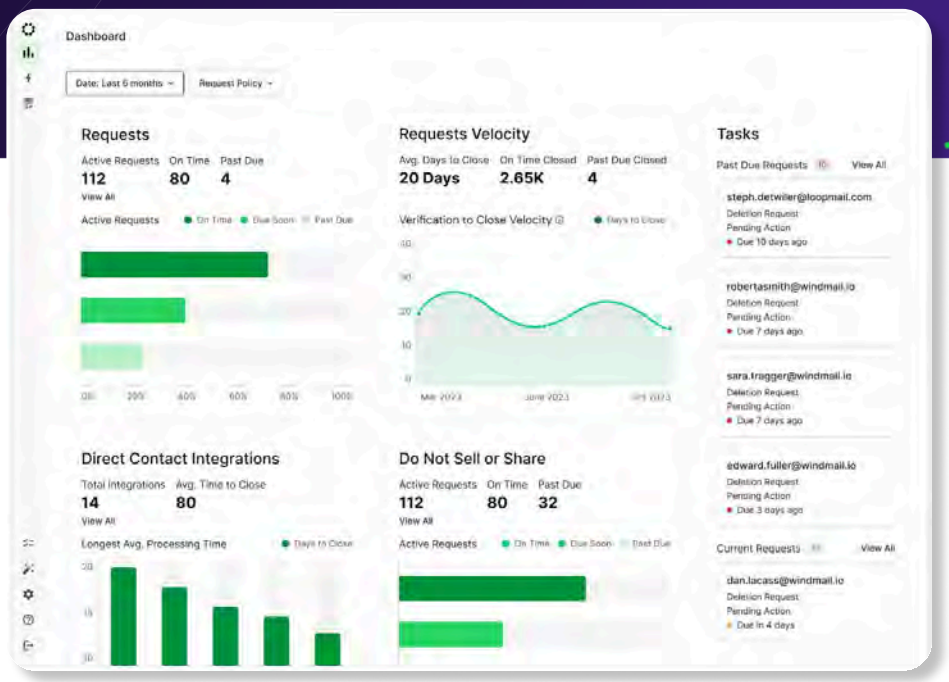
Together, the CCPA and CPRA afford consumers several important rights with respect to their personal information. These right include:

- **Right to Know:** Consumers have a right to know
  - Which categories and pieces of information businesses collect about them;
  - The sources from which the personal information are collected;
  - The purposes for which businesses use their personal information; and
  - Which categories of personal information the business discloses to third parties.
- **Right to Delete:** Except where a business is legally required to keep it, consumers have a right to request that businesses delete any personal information they have collected about them, and request that any service providers to whom they have disclosed it do the same.
- **Right to Opt Out:** Consumers have a right to request that businesses stop selling or sharing their personal information, including via a user-enabled global privacy control.

  If they wish, consumers may subsequently re-authorize businesses to resume selling or sharing their personal information.
- **Right to Correct:** Consumers have a right to request that businesses correct any inaccurate personal information.
- **Right to Limit:** With respect to sensitive personal information, consumers have a right to request that it be used only for limited purposes.
- **Right to Non-Discrimination:** Businesses may not refuse to offer goods or services, charge a higher price, or offer goods or services of a lower quality, to consumers who choose to exercise their rights under the CCPA and CPRA.

First, Cyera's DSPM discovers and classifies personal and sensitive personal data in your IT ecosystem, allowing your organization to create an up-to-date personal data inventory.

Cyera Privacy also enables data subjects to submit requests easily through a structured web form. The form helps automate requests for access, deletion, correction, objection to processing, and transfer of data. Cyera verifies requesters' identities and automatically executes data collection or deletion to securely fulfill the subject access request.

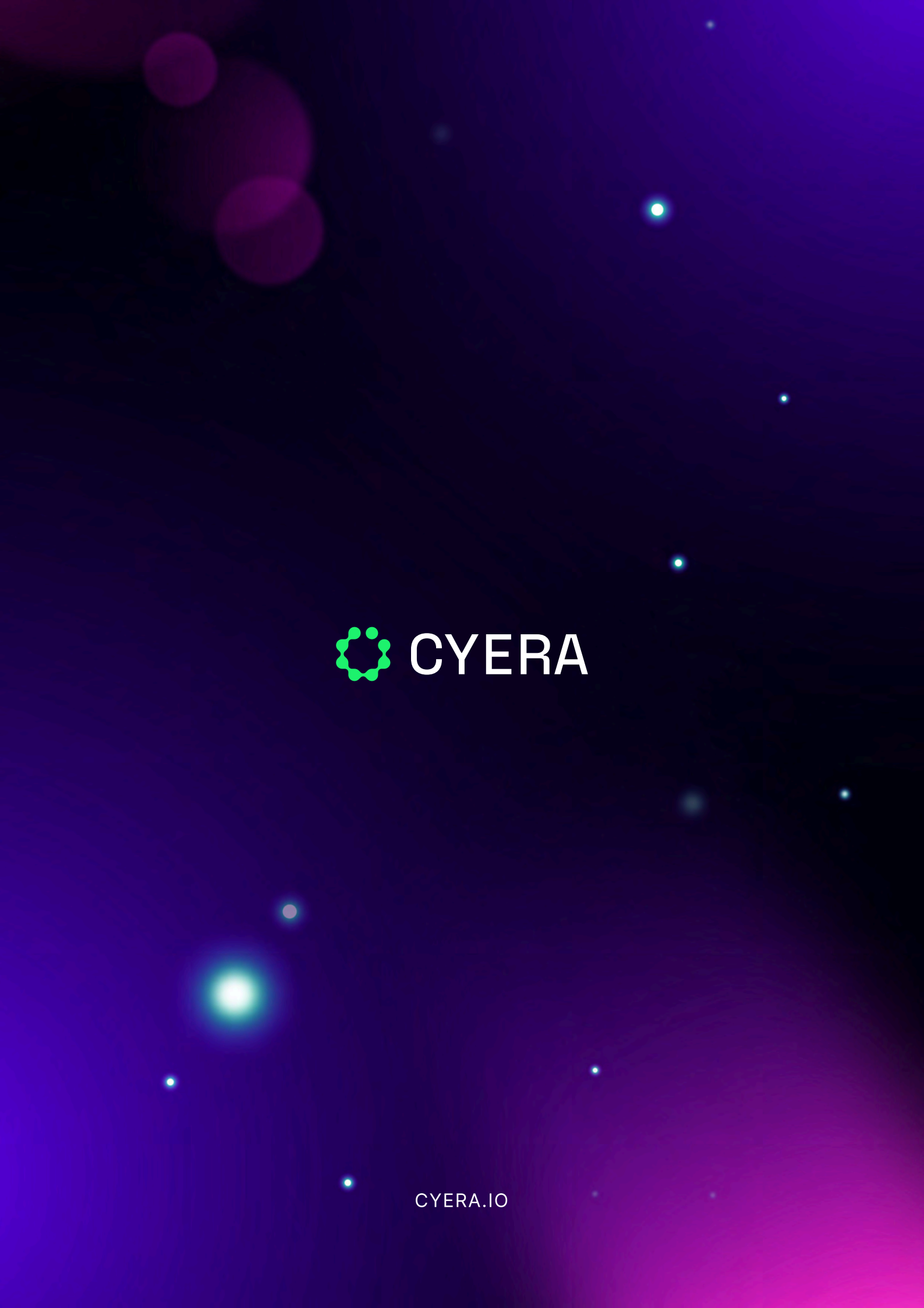


Breach Notification Requirements

The CCPA did not contain its own breach notification rule, relying instead on California's existing Data Breach Notification Law. The latter requires businesses to notify impacted consumers of the date of the breach, a general description of the incident that caused it, and the types of personal information disclosed as a result. In the event the breached data includes identifiers such as Social Security numbers or driver's license numbers, the notification must include contact information for major credit reporting agencies.

In addition, the CPRA established a duty to notify the newly-created California Privacy Protection Agency in the event that a data breach affects more than 500 California residents.

Cyera's data security platform helps your organization simplify breach response by quickly identifying all impacted personal data,including unstructured personal data. It also generates reports and determines the blast radius and materiality of a breach.



CYERA.IO