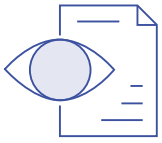
CCPA COMPLIANCE SOFTWARE

The California Consumer Privacy Act (CCPA), similar to the EU's GDPR, allows CA residents to control how businesses handle their personal data. It allows them to request access to, delete, or opt out of sharing or selling their information. Regulatory experts believe this will set the standard for data privacy within the US and become a benchmark framework for data compliance.

CCPA compliance standards are still evolving. In November 2020, CA voters approved the more comprehensive California Privacy Rights Act (CPRA, commonly referred to as the CCPA 2.0) which expands privacy protections, as well as the obligations of organizations that process personal information. starting January 1, 2023.

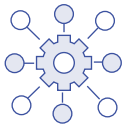
Under CCPA, organizations need to know exactly what PII data they possess, where it resides, and how it's secured. individuals can sue businesses for non-compliance, up to $2,500 per violation (under CPRA, the California Privacy Protection Agency (CPPA) may also impose fines). And while fines may be insignificant if the number of violations is low, loss of customer trust can devastate your brand and shareholder value.

HOW GROUND LABS CAN HELP ENSURE CCPA COMPLIANCE

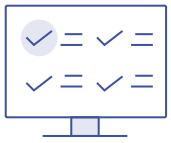


Scan for over 300 different types of structured and unstructured data including pre-configured,CCPA-specific PII patterns.

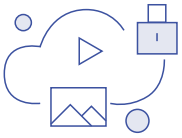
Demonstrate CCPA and CPRA compliance with custom reporting and analytics available in the Enterprise Recon dashboard.



Accurately map data across networks, servers, and platforms to keep tabs on PII and more easily respond to consumer requests.

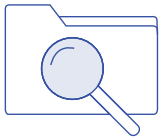


Easily build custom data types and search platforms to locate and remediate unique data types to address your organization's unique CCPA and CPRA needs.

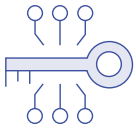


Search within both structured and unstructured data sources including servers, on desktops, email, and databases, on prem and in the cloud.

Reduce the overall time and investment required to reach and uphold CCPA and CPRA compliance, even as regulations change over time.



Search across the entire organization with support for Windows, macOS, Linux, FreeBSD, Solaris, HP-UX, IBM AIX and much more.



Execute a proactive approach to data security - as opposed to a reactive approach that relies on damage control post-breach - to build a stronger foundation of trust within your organization.

Book a complimentary sample data analysis with Ground Labs at https://go.groundlabs.com/book-a-demo

GROUND LABS

CALIFORNIA PRIVACY RIGHTS ACT (CPRA): WHAT TO KNOW

What Has Change Under the CPRA?

While the CPRA won't take effect until 2023, the law builds on the foundation of the CCPA and aims to enhance consumer privacy protections, as well as the obligations for companies and organizations that process personal information. Here are some specific changes to pay attention to:

- Employee and Independent Contractor Data: Under the CPRA, the obligations of organizations to protect the privacy rights of their employees and independent contractors is delayed until January 1, 2023.
- Redefining of Key Words: Redefinition of key words that focus on the meaning and scope of "business" and "breach" to remove some of the ambiguity in the law.
- Establishment of California Privacy Protection Agency: The CPPA will be the first agency in the US dedicated solely to privacy. Comprising a five-member board, with expertise in privacy and data security, the CPPA will be in charge of providing guidance to businesses and consumers.
- Power of the CPPA: The CPPA will have the authority to prevent future attempts by businesses to avoid or not comply with the CPRA, as a result of lobbyists' attempt to weaken the law.

GDPR Concepts the CPRA will Introduce

The CCPA is referred to as the "American GDPR" and with the implementation of the CPRA, the following concepts will be introduced:

- Right to Rectification: Consumers will have the explicit right to request that organizations correct inaccurate information.
- Right to Restriction: The CPRA grants consumers the right to limit the use and disclosure of their sensitive personal information, and businesses must notify a consumer if they intend to use it beyond specified purposes.
- Sensitive Personally Identifiable Information: Not all personally identifiable information (PII) will be treated equally under the CPRA, as it introduced a new category of data known as "sensitive personal information," which applies to log-in credentials, financial account information, precise geolocation, contents of certain types of messages, genetic data, racial or ethnic origin, religious beliefs, biometrics, health data, and data concerning sex life or sexual orientation, etc..

How Business Should Prepare for the CPRA

For businesses now looking to prepare for the CPRA implementation date, there are several steps to take. For starters, organizations will need to know if they are subject to the provisions within the CPRA. A good rule of thumb is that if your organization is subject to the CCPA, then you likely will also need to achieve CPRA compliance.

Next, know the key dates. Organizations will need to achieve CPRA compliance by July 1, 2023. But organizations should also keep in mind that the CPRA has a "look back" clause that applies to all data collected starting on January 1, 2022. So starting your compliance journey early and effectively will be critical to avoiding falling victim to this look back period.

And of course, businesses looking to achieve CCPA compliance and prepare for the CPRA must have the right tools in place to ensure compliance, starting with data discovery. By taking a no-assumptions based approach, through data discovery organizations will have a more holistic view of their data management strategies and locate missing or sensitive data.

Ground Labs' premier and award-winning data discovery software Enterprise Recon is able to detect over 300 types of structured and unstructured data, including CCPA-specific PII patterns. With the ability to map data across networks, servers, and platforms and demonstrate CCPA and CPRA compliance with custom reporting, your organization can proactively prepare for any data security challenge that comes your way.