



Ongoing CCPA Compliance Made Easy

CCPA is a law designed to protect the data privacy rights of citizens living in California. How can you ensure your employees use sensitive data safely?

Personal data under CCPA is defined as:

- Direct identifiers such as real name, alias, postal address, social security numbers, driver's license, passport information and signature;
- Indirect identifiers such as cookies, beacons, pixel tags, telephone numbers, IP addresses, account names;
- Biometric data such as face, retina, fingerprints, DNA, voice recordings, health data;
- Geolocation data such as location history via devices;
- Internet activity such as browsing history, search history, data on interaction with a webpage, application or advertisement; and
- Sensitive information such as personal characteristics, behavior, religious or political convictions, sexual preferences, employment and education data, financial and medical information.
- In addition, under CCPA, personal information has no format or medium limitation, which means that even pictures or sounds can qualify as personal information, if they fall under the definition in the law.

HOW DASERA CAN HELP

- Dasera **finds where sensitive data resides** in the data warehouse. Dasera automatically crawls, samples, and classifies sensitive data.
- Dasera enables data security professionals to **supervise the tagging of sensitive data**. The data security team can re-categorize data as necessary; remove any sensitive data false positives; and manually mark any sensitive tables/fields that Dasera's scan may have missed.
- Dasera automatically **propagates sensitive data tags** to derivative tables. Because Dasera is monitoring each and every query in the data warehouse, it can automatically -- either retroactively or in real-time -- tag fields that incorporate sensitive data from other tables.
- Dasera **can execute a full deletion** of the consumer's personal data in the data warehouse, because Dasera knows all locations of sensitive data in the data warehouse.
- Dasera policies can be customized to **restrict third parties' access to data** for consumers who have opted out of third-party data access.
- Dasera is hosted software. As such, Dasera achieves all the above **without copying any personal data to external servers**, ensuring compliance with CCPA

"[Dasera] is by far the best architecture I've seen for this type of product. We've wanted to adopt this approach for a while."