CallRail & California Consumer Protection Act (CCPA)

Give each customer access to and control over their personal data

CCPA (California Consumer Protection Act) is California's ground breaking privacy law that provides data protection of any personal information to California residents. So what's considered personal information under CCPA regulations?

Personal information is any information that can be directly or indirectly tied to an identified or identifiable individual or their household, such as:

- Name
- Phone number
- Social security number
- Email address
- Location data
- Protected health information
- Postal address
- Driver's license
- IP address
- Cookie identifier
- Religious
- Political affiliation

It does not, however, cover any information that is a matter of public record such as federal, state, or local government records.

Businesses that need to aim for CCPA compliance

The CCPA applies to any businesses that collect personal information from California residents and meet at least one of the following:

- Has annual gross revenues of $25 million
- Collects or sells the personal information of 50,000 or more consumers, households or devices
- Obtains 50% or more of its annual revenues from selling consumers' personal information

While smaller businesses are given some flexibility with CCPA since they don't qualify as major offenders, any business that handles sensitive data from California consumers needs to aim for compliance.

How CallRail helps businesses stay CCPA compliant

CallRail helps businesses and marketers make data informed decisions by not only capturing the marketing campaign and source that drives each phone call and form submission, but capturing insightful data into how each call is handled.

That's a lot of customer data. And for businesses interacting with California customers and prospects, they need to ensure CCPA compliance.

Our promise to CallRail customers: your data is in your hands

First and foremost, you have the right to know how your personal information is collected, used, and stored. As a service provider for your business and customers, the data we collect is not sold or shared outside of our services.

We may, however, use the information you provide through our platform to:

- Personalize your customer experience
- Make improvements to our sites and marketing campaigns
- Send personalized emails regarding CallRail promotions, events, and updates

You can read more about how we collect and use data within our privacy policy.

Most importantly, if you wish to stop the collection and use of your data, you have control over your privacy rights. **You have the right and ability to access your data, port your data out of CallRail, and request that your data be erased.**

California cookie consent
For all California residents, a cookie banner will be displayed at the bottom of the webpage for you to interact with. From this banner, you'll be able to control which cookies to allow or disallow. It is important that if you choose not to interact with the cookie banner, it is assumed that you consent to our cookie policy.

Maintaining individual rights

Both you and those who interact with your business have the right to be informed of how your personal information is collected, used, and stored. You, as an individual, also have the right and ability to access your data, port your data out of CallRail, and request that your data be erased. California customers can submit a request to privacy@callrail.com or call CallRail Support at +1 (888) 260-7523.

PII/PCI Redaction

All Personal Identifiable Information is automatically redacted from call recordings and call transcripts once PII Redaction feature is activated.

All data encrypted “in transit”

All access to CallRail is encrypted via SSL to protect data from interception on network points between the user and CallRail.

All data encrypted “at rest”

All call records, web visitor sessions, and call routing data are fully encrypted when stored on disk. This data is seamlessly decrypted as-needed for reporting purposes when accessed by the customer. These precautions protect the data even if hard drives fail, or are decommissioned or stolen.

Secure access

Individual users are granted their own login credentials, which can be controlled by an administrator. Login sessions automatically expire after a brief period of inactivity to prevent unauthorized access.

Firewalls and private network gaps

The databases, application servers, and other machines responsible for routing calls through CallRail are isolated and inaccessible via the public internet (except the web application itself, of course). This private network is protected by a pair of redundant hardware firewalls to ensure only expected traffic is allowed.