

CallRail & General Data Protection Regulation (GDPR)

Give each customer access to and control over their personal data

GDPR (General Data Protection Regulation) is the latest set of rules in the European Union governing how personal data can be used and stored. So what all is considered personal data?

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

- Name
- Phone number
- Email address
- Company information
- Job title
- Location data
- Protected health information
- IP address
- Cookie identifier
- Religion
- Political affiliation

Businesses that serve EU citizens and collect any of the sensitive data above have a legal obligation to inform users of what information is collected and for what purposes. EU users must then consent to the collection and use of their data by opting in, but also be given an easy way to opt out and take their data with them.

How CallRail helps businesses stay GDPR 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 European customers and prospects, they need to ensure they're achieving GDPR compliance.

Out of the box, CallRail is GDPR compliant. The roles of those interacting with customer data are split two ways:

1. **Data controllers:** Data controllers determine the purposes and means of processing personal data that is collected and stored.
2. **Data processors:** A data processor processes personal data on behalf of the controller.

Our promise to CallRail customers: you rule your personal data

First and foremost, you have the right to know how your personal data 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.

EU cookie consent

For all citizens within the European Union, an overlay will appear on our website that requires you to interact with a cookie banner. From this banner, you can control which cookies to allow or disallow. Unfortunately, if you do not interact with our cookie banner, you will not be able to access our site or our services.

Maintaining individual rights

Both you and those who interact with your business have the right to be informed of how your personal data 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](#). As additional options, EU customers can email privacy@callrail.com or call CallRail Support at +1 (888) 260-7523.

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.