Calabrio

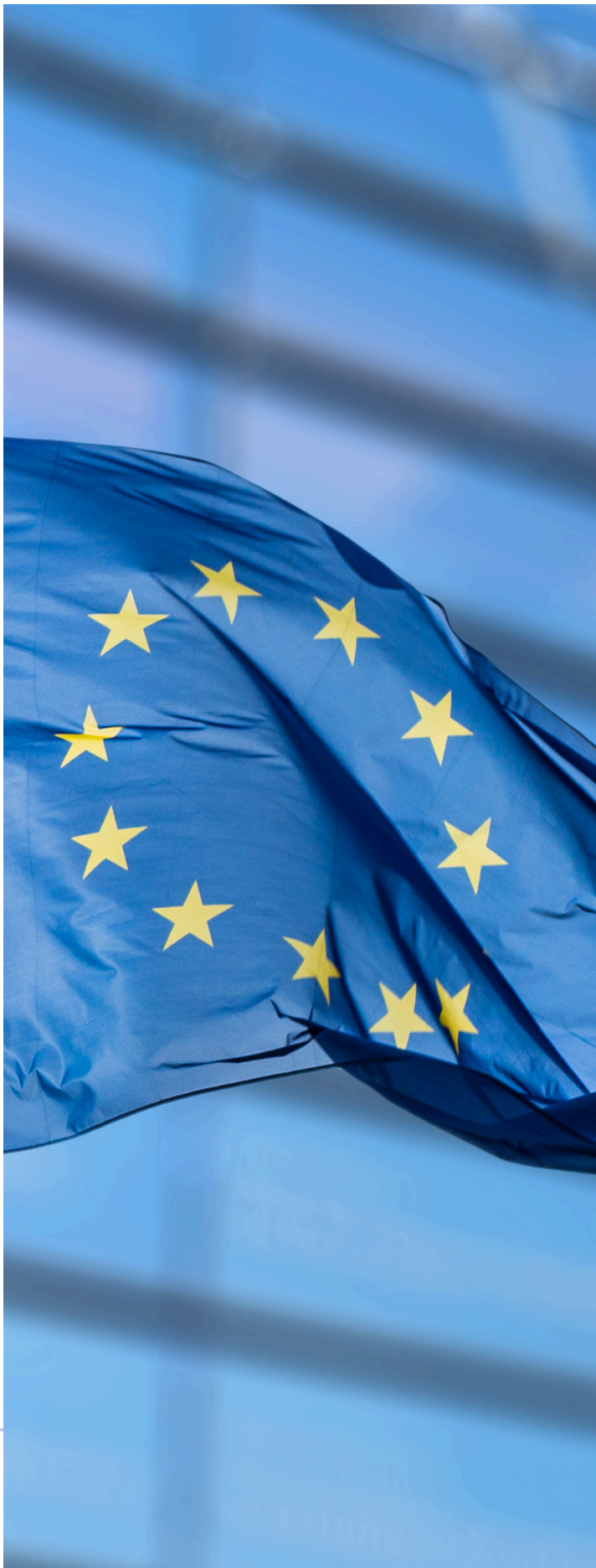
Calabrio's "How-To" Guide on Navigating the GDPR and CCPA

2025

On May 25, 2018, the **General Data Protection Regulation (GDPR) was put into effect by the European Union (EU)** to strengthen and unify data protection for all individuals within the EU. The law affects any company that markets to an EU citizen, regardless of where the organization or citizens are located. Under the GDPR, if you have even one EU contact within your contact center database, you may need to understand and comply with the GDPR and its requirements.

On January 1, 2020, the United States, within the State of California, enacted California Assembly Bill No. 375, dubbed the **California Consumer Privacy Act (CCPA)**. This act is similar to the GDPR, providing for the confidentiality of personal information in various contexts and requiring disclosure of any breach of security of computerized data that includes personal information. After January 1, 2020, companies will have 30 days to comply with the California regulation once notified that they are in violation.

Calabrio is here to help you understand and navigate both the GDPR and CCPA. In this brief summary, we examine security risks and explain how Calabrio can help your organization comply with and maintain GDPR and CCPA requirements.



SECTION 02

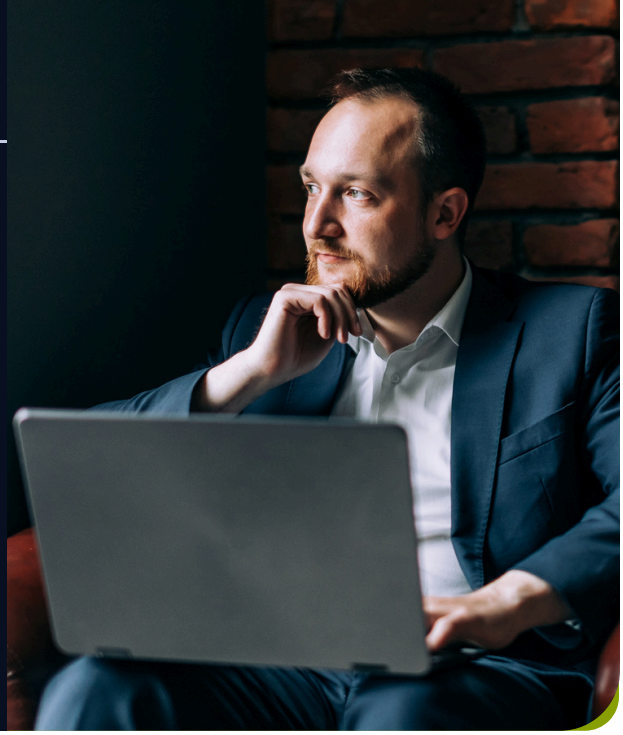
BASICS UNDER THE GDPR

Within the EU, the GDPR strengthens the rights of EU citizens to know how and why companies collect and use their personal data — and to choose whether companies can do either in the first place. The GDPR increases the responsibility of companies to protect the personal data they do collect and alert customers of any data breaches. The GDPR also makes non-compliance much more painful — companies that don't comply face fines of up to 100 million euros or four percent of the business's annual revenue, whichever is higher. The primary goals of the GDPR are to give control of personal data back to EU citizens and residents, unify regulation within the EU and simplify the international business regulatory environment. In a concept known as "privacy by design," privacy and data protection become part of a company's core requirements with the GDPR the way in data collection and storage.

Under the GDPR, organizations are required to:

- implement "Privacy by Default" and "Privacy by Design";
- maintain appropriate data security;
- notify data protection agencies and consumers of data breaches;
- obtain appropriate consent for most personal data collection and provide notifications of personal data processing activities;
- obtain a parent's consent to collect data for children under 16 as a general rule, though age of consent may differ by country. **More information can be found here;**
- keep records of all processing of personal information;
- appoint a data protection officer (conditions apply); assume responsibility for the security of processing of personal data by designated business partners;
- conduct data protection impact assessments on new processing activities;
- institute safeguards for cross-border data transfers;
- consult with regulators before completing certain processing activities; and be able to demonstrate, at any time, on demand, compliance with GDPR.

WHAT RIGHTS DOES THE GDPR GIVE EU CITIZENS?



The GDPR law significantly expands an individual's rights over their personal data, which also significantly expands your responsibilities as a contact center. At a high level, here is an explanation of the law and the expanded rights it gives EU citizens around "consent."

- **Right to be informed.** The GDPR gives individuals the right to be informed about the collection and use of their personal data.
- **Right to restrict processing.** Under certain conditions the GDPR allows individuals to "block" or suppress the processing of their personal data to protect against illegitimate usage. More information can be found here.
- **Right to object.** With the GDPR, the individual has the right to object to the processing of their personal data unless you can demonstrate legitimate grounds for processing.
- **Rights in relation to automated decision making and profiling.** The GDPR provides protection for individuals against systems that make decisions solely by automated means and against the automated processing of personal data to evaluate certain things about an individual.
- **Right of access.** With the GDPR, you need to be able to locate every piece of an individual's data stored within your workforce optimization (WFO) system and communicate how it has been used, whenever an individual requests that information.
- **Right of rectification.** The GDPR empowers individuals to request corrections to any of their personal data, so your contact center agents and other system administrators need easy ways to find, update and document these changes.
- **Right to erasure (the "right to be forgotten").** The GDPR also empowers individuals to request the deletion of all data gathered about them — and you'll need to comply if the data is no longer needed to achieve its original purpose or your legal basis for gathering it was the individual's consent.
- **Right of data portability.** The GDPR enables individuals to request their personal data in a commonly used format, like CSV or XLS, which they then can reuse for any purpose across different services.

BASICS UNDER THE CCPA:

The primary goal of the CCPA is to help Californians properly protect and safeguard their privacy. Like its European counterpart, the CCPA grants consumers the right to request the disclosure of specific pieces of personal information from a business. The CCPA requires businesses to make disclosures about the information itself and the purposes for which that information is being used. Also, it allows Californians to demand their personal information from third parties as well.

After January 1, 2020, companies will have 30 days to comply with the California regulation once notified that they are in violation. If the problems are not resolved, the state may issue fines of up to $7,500 per record. Also, for the first time, the individual may sue companies for non-compliance if they choose to ignore the regulation.

WHAT RIGHTS DOES THE CCPA GIVE CONSUMERS?

Through the CCPA, the California Legislature seeks to further Californians' right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights:

Right to be informed. A consumer shall have the right to request the disclosure of all personal information collected by a business, including categories and specific pieces as needed. Likewise, any business that collects the consumer's personal information shall, at or before the point of collection, inform the consumer that their information is being collected and specify a valid reason. A business may not collect information without notifying the consumer.

Right to be forgotten. A consumer shall have the right to request that a business delete any personal information that has been collected. A business that receives a verifiable request to delete the consumer's personal information shall delete the information from its records, unless there is a valid, legal reason to maintain the information. The following are considered valid, legal reasons:

- to complete the transaction for which the personal information was collected;
- to detect security incidents or otherwise protect against fraudulent or illegal activity;
- to debug, identify and repair errors that impair existing functionality;
- to exercise free speech;
- to comply with California Electronic Communications Privacy Act;
- to engage in research;
- to comply with legal obligations;
- to otherwise use the consumer's information internally, in a lawful manner compatible with the context in which the consumer provided the information.

Right of Disclosure. A consumer shall have the right to request the following disclosures from any business that collects personal information:

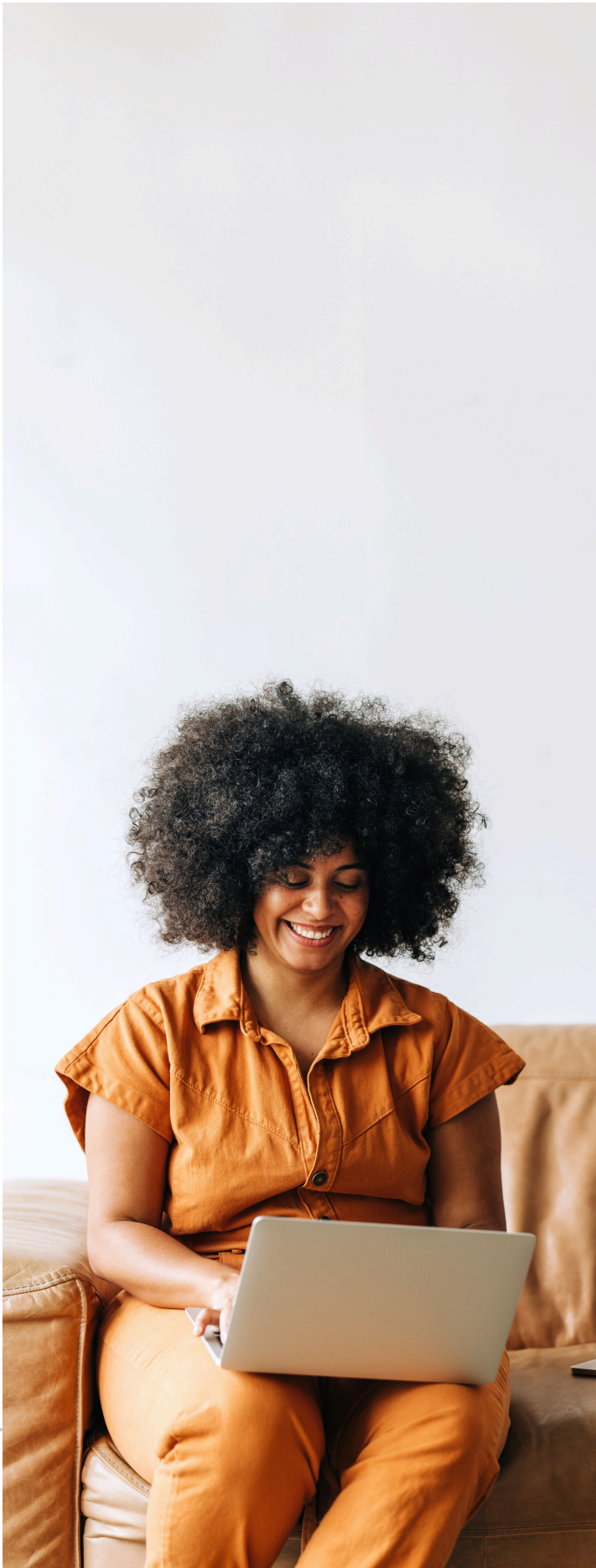
- categories of personal information it has collected about that consumer;
- categories of sources from which the personal information is collected;
- business or commercial purposes for collecting or selling personal information;
- categories of third parties with whom the business shares personal information;
- specific pieces of personal information it has collected about that consumer.

Right to opt out. A consumer shall have the right, at any time, to direct a business not to sell the consumer's personal information to third parties. A business that sells consumers' personal information to third parties shall notify the consumer that this information may be sold, and that the consumer subsequently has the right to opt out of the sale of their personal information. A business that has received direction from the consumer not to sell their personal information shall be prohibited from doing so. A business also shall not sell personal information if the business has actual knowledge that the consumer is less than 16 years of age.

Right of Non-Discrimination. A business shall not discriminate against a consumer for exercising any of these rights. Retaliatory actions prohibited by the law include:

- denying goods or services to the consumer;
- charging different prices or rates for goods or services; providing a different level or quality of goods or services to the consumer;
- suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

Like its European counterpart, the CCPA grants consumers the right to request the disclosure of specific pieces of personal information from a business.



SECTION 02

HOW CALABRIO CAN HELP

Calabrio offers many out-of-the-box capabilities related to capturing, viewing, deleting and protecting employee and customer information that can help you comply with GDPR and CCPA.

We help contact centers comply with the above mandates by providing advanced data capture, data viewing, data deletion and data protection capabilities that support an employee or customers' right to control their personal data. Additionally, our consultants can work with you to ensure your Calabrio solution is designed to comply with regulatory requirements that fit within the framework of the Calabrio Shared Responsibility Model.

Data Capture

Our solutions can capture the following personal data in text form or sync this data from the automated call dialer (ACD) or other contact center systems:

- Agent or user first and last name
- Agent ID
- Title, position and organizational belonging
- Competence
- Data related to scheduling and reporting
- Contact information (company, email, phone, physical business address)
- Custom metadata options

We also can capture during recorded calls the following personal data:

- Agent or user first and last name
- Caller information including name, email address and account information

We will work with you based on your unique environment to address handling personal data, along with methods to document and report explicit consent.

Data Viewing

When a customer or employee requests their personal data, Calabrio's basic and advanced reporting solutions — along with ad-hoc export capabilities — can help you quickly retrieve data in an easily viewable format. Our system-wide auditing and reporting also can identify key system changes or updates.

Data Deletion or Anonymization

You can create a workflow within your Calabrio solution to delete and purge an individual's data and associated records — including removing all identifiable data[1]— whenever they make a request. Alongside Calabrio solutions, you can use your internal policies to ensure employee information is anonymized at the time of entry.

Data Protection

Calabrio leverages a variety of industry standards and best practices to protect customer and employee data: [2]

- **End-to-End Encryption -** An individual's data — including recordings — captured by Calabrio is encrypted at the source, in transit and at rest, at no additional cost using Advanced Encryption Standard (AES).
- **Restricted Access -** Calabrio restricts access to the recordings using role- based access controls.
- **Security Best Practices -** The Calabrio security program is based on industry leading frameworks such as the NIST Cyber Security Framework and the Center for Internet Security Critical Security Controls. Calabrio has obtained the SOC2 Type 2 certification annually since 2017.
- **PCI Compliance -** As a Service Provider, Calabrio is PCI compliant, as attested to by an independent Qualified Security Assessor (QSA).
- **ISO Certification -** Calabrio has obtained the ISO 27001 certification for its Support Services department.

1 The Calabrio customer must implement appropriate processes and procedures for purging data. Data is not redacted; it is purged through workflow rules.

2 The Calabrio customer must implement appropriate processes and procedures in order to be compliant. For step-by-step instructions on how to respond to data privacy requests in Calabrio products, please refer to the product user documentation.

LEVERAGE CALABRIO ANALYTICS TO MITIGATE RISK

Calabrio Analytics includes speech, desktop and text analytics — providing a holistic view of customer interactions. With Calabrio Desktop Analytics supervisors know exactly what's happening at agent desktops — including what the agent is seeing, what windows are open, what's being typed, etc. Speech analytics then looks for context within the verbal conversations these agents are having with customers. These two data streams give businesses unprecedented visibility into individual agent behavior so that best-practice work habits, including script compliance and the effective use of software applications, can easily be reinforced and replicated across the contact center.

Calabrio is the customer experience intelligence company that empowers organizations to enrich human interactions. The scalability of our cloud platform allows for quick deployment of remote work models — and it gives our customers precise control over both operating costs and customer satisfaction levels. Our AI-driven analytics tools make it easy for contact centers to uncover customer sentiment and share compelling insights with other parts of the organization. Customers choose Calabrio because we understand their needs and provide a best-in-class experience, from implementation to ongoing support.

© Copyright 2022, Calabrio, Inc. All rights reserved. Calabrio and the Calabrio logo are the registered trademark of Calabrio Inc. All other products are the property of their respective companies.