



HANDBOOK

CCPA Guide for Businesses

Understand the CCPA laws and use these 6 steps to implement a privacy strategy that ensures continuous compliance without manual processes or extra overhead for your team.

datagrail.io



CCPA Guide for Businesses

In effect as of January 1, 2020, the CCPA creates many new compliance requirements for businesses.

Having a solution that provides continuous compliance and can map personal data is important for a successful privacy approach. This handbook answers common questions about CCPA and shares best practices for your organization.

Contents

- PART ONE [Understanding the CCPA](#)
- PART TWO [Six steps to CCPA compliance](#)
- PART THREE [CCPA Resource round-up](#)

Published March 2020. Disclaimer: privacy laws are quickly evolving and this information is subject to change as regulations are updated.



Understanding the CCPA



Overview: What is the CCPA?

Consumer rights

Effective January 2020, the updated California Consumer Privacy Act gives new data protection rights to California residents broadly similar to those granted to Europeans by the GDPR, including:

1. The right to know what personal information a business has collected
2. The right to delete that information
3. The right to know whether personal information is sold or disclosed and to whom
4. The right to say no to the sale of personal information
5. The right not to be discriminated against for exercising the aforementioned rights

Businesses Affected

Businesses with an excess of \$25 million in revenue, with 50,000 or more instances of personal data, or businesses that make more than half their revenue from the sale of personal data.

Data Reporting

Reporting for data breaches and data processing practices are also regulated by the CCPA. These reports must be maintained for a minimum of two years beyond each request.

Personal Information

Companies will be responsible for personal information dating back to January 1st, 2019, due to the 12-month “look back” period.

Identity Verification

CCPA requires up to 3 levels of identity verification depending on the type of request, yet discourages businesses from collecting more PII (Personally Identifiable Information) during the verification process. Identity verification requires strict controls to prove the requestor is actually the person in your system. Consider how your organization will manage this requirement at scale while building out your privacy program.

Best Practices to Prepare

1. Determine an efficient workflow for processing upcoming right to know, right to say no, and deletion requests.
2. Prepare a request intake and response process to manage personal data.
3. Create a process for user verification for requests. Consider a platform that helps you use existing data in your systems to verify privacy requests from your consumers without asking for further personal data.
4. Ensure consumers are comfortable with how their data is used and how their communication preferences are handled.
5. Provide confirmation and validation of required activities and processes upon audit.
6. Compile required information including to whom data is sold, and provide an option for users to opt out of their data being sold on your website.

Why should your business care?

As of January 1st, 2020, companies will have 45 days to meet all regulation requirements and become prepared to handle and answer right to know and right to say no requests. If businesses fail to comply with the regulation, fines of up to \$2,500 will be imposed on each case, per individual or person. The law will be enforced by the Attorney General and will allow for private right of action by consumers in certain cases. CCPA also requires companies to maintain records of all consumer privacy requests and how the business responded for at least 24 months.

Find out why companies like Overstock, Restoration Hardware, Plexus, Crunchbase, ZoomInfo and more have chosen DataGrail as their CCPA platform.

[Learn More](#)

Six steps to CCPA compliance



Six steps to CCPA compliance

The [California Consumer Privacy Act \(CCPA\)](#) is the first major piece of United States privacy legislation, but it won't be the last.

There are already similar bills in the works in Washington, New Jersey, New York, Hawaii, Massachusetts, New Mexico, Rhode Island, and Maryland. Introduced on June 28, 2018, the CCPA adopts much of its framework from the European Union General Data Protection Regulation (GDPR) - although there are some subtle differences. For example, the CCPA extends its protections to households and devices, not just individuals, and includes the right to opt-out of the sale of personal information.

If there is one lesson we learned from the May 25, 2018 GDPR deadline, it is that companies did not give themselves enough time to prepare. Anecdotally, we witnessed the public-facing work to update privacy policies and implement cookie banners, but was the same attention given to the tedious (and often manual) task of preparing data inventories behind the scenes? Are companies equipped to process consumer privacy rights requests like the right to deletion?

Our [research](#) suggests a lot of companies were blindsided by how much time and money it takes to sustain compliance. Now that the California Consumer Privacy Act is in effect as of January 1, 2020, make sure your team has a sustainable compliance program in place. Here's how...

Update Your Privacy Policy

One of the first steps toward CCPA compliance is to update your privacy policy.

Similar to the GDPR, the CCPA requires companies to disclose what type of data is being collected and the purpose of its collection; however, there are some subtle differences that may require separate policies for California consumers and European citizens. For the CCPA, protected data includes personally identifiable information, commercial data/sales transactions, internet activity, biometric data, geolocation data, employment data, educational data and metadata.

Implement a Notification Banner

Hand-in-hand with an updated privacy policy, companies should be planning to implement a notification banner.

This isn't a requirement of CCPA but it is best practice to inform users of your compliance with the CCPA and whether you plan to sell any personal data you collect so they can opt-out.

It's important to recognize that updating your privacy policy and implementing a notification banner are only the start of compliance: readiness. Sustained compliance can be much more challenging to achieve.

Build Your Data Inventory

Sustained compliance is an ongoing process that requires granular visibility into dynamic business systems.

It's not uncommon for a [Fortune 500 company to have more than 100 business systems that contain personal data](#), each operating independently. You could build your data inventory through manually-conducted surveys and questionnaires, but these static lists are time-consuming, error prone, and are immediately outdated - especially without an additional process to update them when new systems come online. Companies that seek to implement a sustainable compliance program should consider solutions that enable them to integrate business systems to streamline response to California consumer privacy rights.

Establish a Workflow to Respond to Consumer Rights Requests

04

Responding to California consumer privacy rights could introduce a second tedious process if your company has not prepared by integrating its business systems.

The manual response to manage these privacy requests requires complex data inventories to inform multiple system owners of the data that needs to be deleted. This can become a rather expensive process since legal counsel is frequently employed to manage these requests.

Hard Deletes Aren't Easy

05

One potential pitfall when responding to the right to be deleted is the difference between a hard delete and a soft delete.

A soft delete, such as removing information from a dashboard, does not necessarily mean it has been deleted from your service provider. A hard delete will typically require an email to your service provider to ensure this data has been deleted, both by them and by their sub-service providers.

You'll want to blacklist records that have been deleted to avoid them being reintroduced to your database in the future.

Again, this can become a tedious manual process when business systems have not been integrated.

Third-party Providers, All on One Page

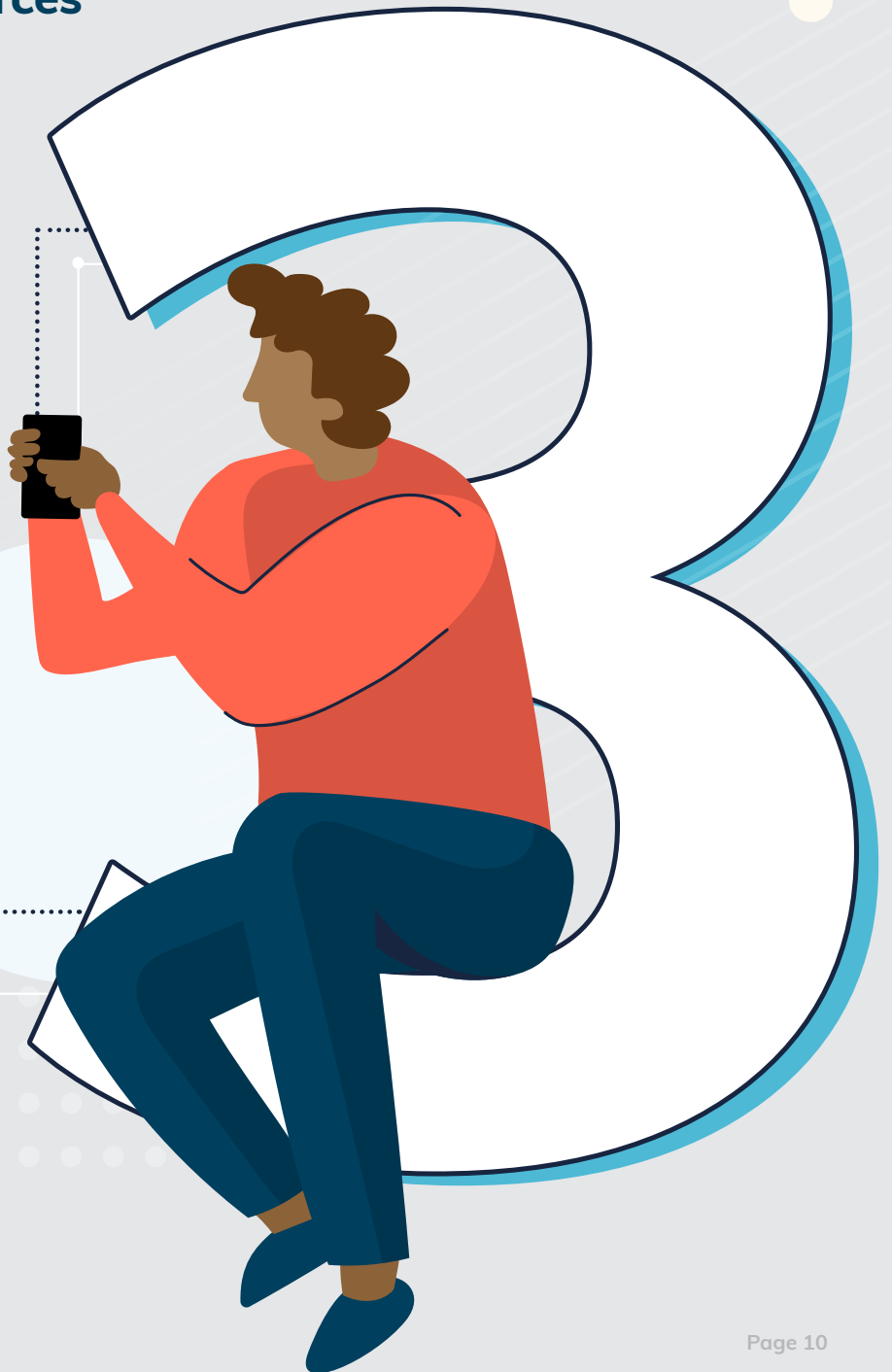
06

As evidenced by the complexity of managing hard deletes, it is critical to ensure that third-party service providers and partners that store protected data have also implemented a sustainable compliance model.

Implement contractual obligations, such as a data privacy agreement, to ensure your partners are working toward the same standards as your company. And reconsider working with your service providers if they have not completed their associated data inventories or are unable to integrate with your business systems. The last thing you want is for your company to be penalized because of a mistake by your partners.

Want more?

Here's a round-up of our
top CCPA resources



Recommended reading

With the CCPA now in effect, and enforcement on the way, we wanted to share with you some of our top resources on the legislation. These range from expert opinions and predictions to interpreting some of the more challenging parts of the regulation.

[20 Questions on the CCPA with Answers from Privacy Experts](#)

There remains confusion around CCPA, particularly in how it compares to GDPR, what's covered under CCPA and who must comply. To help you better understand the CCPA basics, we asked data privacy experts.

[The CCPA Sees New Changes and Regulations by Attorney General](#)

Two months from implementation, California's Attorney General finally released the long-anticipated draft regulations for the CCPA.

[Preparing for CCPA's Section 2 - Consumer Rights](#)

CCPA is fast approaching. As of this writing, organizations have less than three months to prepare for the new data privacy law.

[GDPR Chapter 3: Where Are We Now & How Can We Use It to Prepare for The CCPA](#)


Chapter 3 of the GDPR and Section 2 of the CCPA have some of the most challenging requirements for businesses. Find out how to comply here.

[Data Privacy Changes Coming to California in 2020](#)

On March 22, The Berkeley Center for Law and Technology hosted a forum to discuss data privacy laws around the world and the upcoming CCPA.

[CCPA Public Forum \(San Francisco\): 10 Topics & Comments](#)

The California Dept. of Justice held its first of six public forums on the CCPA. See what concerns and comments were conveyed by the public.



DataGrail helps companies comply effortlessly with existing and emerging privacy laws, such as GDPR and CCPA.

With over 200 pre-built connectors currently in place, the DataGrail platform provides a 360-degree, real-time view of the applications used and maps the personal data associated with each of those systems. DataGrail also allows customers to manage their privacy request workflows and email preferences across applications.

[Request a demo](#)