ETHYCA

9 Steps to Getting Privacy Right

for the CCPA & Beyond

The California Consumer Privacy Act is the first major piece of data privacy legislation in the United States. But it won't be the last.

SME teams wondering how to implement best privacy practice can be intimidated by the prospect; there's lots to tackle and lots of considerations to be made.

This guide contains three groups of three steps that any team can undertake to begin modernizing their data privacy operation. Take these steps and you'll be well-positioned for CCPA and the many upcoming regional, national, and international pieces of privacy legislation in the pipeline.

Data Discovery & Access

First, understand where your data lives and how to find it.

Identify the Data You Hold

Mapping your data is an essential first step for dealing with privacy regulations. Get key team members in a room and draw up a schema for where in your business you collect, store, and process customer data.

The deliverable from this exercise is most often a visualization showing various points of data activity as a nodal network called a Data Map. Armed with a comprehensive Data Map, teams can act confidently when required to access data points from their system.

Build Processes for Data Discovery & Retrieval

Once your data has been mapped, the next step is understanding how you can retrieve individual data records from across the full suite of data platforms your team uses. This is often a significant resource problem that platforms like Ethyca exist to solve.

It's vital to consider differences in data structures across different data platforms, and how those impact your ability to build a comprehensive record of a customer that can be quickly retrieved. Given the messy nature of data collection and storage for most SMEs, building a system for efficient retrieval is often the biggest challenge in building a solid privacy operation.

Set A Process for Handling Consumer Access Requests

Once you're confident in the ability to retrieve the data you need, the last piece of the puzzle is setting a workflow for when consumers make requests pertaining to their data records. CCPA gives a business 45 days to respond to such requests.

Separate from the actual process of retrieving the data, a business will need to designate a team member to oversee the inflow of Consumer Requests, communicate when requests have been received, undertake the necessary data actions, and provide the consumer with confirmation their Request has been completed.

Considering Consent & “Do Not Sell”

Next, re-examine the way your business handles customer consent.

Review Treatment of Consent Preferences

Laws like the CCPA give consumers greater power to selectively grant or deny consent to data usage. Teams need a streamlined system for implementing user consent updates across a range of business activities in consistent, efficient fashion.

They also need to consider the customer experience. If a user wants to opt out of receiving all marketing-related communications, it shouldn’t take a journey across multiple web properties to enact this choice. Consider building a centralized location where any user can manage all consent preferences related to the business.

Build a *Do Not Sell* Button

This provision is unique to the CCPA and a very visible sign that you’re taking user privacy seriously. This button must be located on your website’s homepage, and users must be able to file a request without creating an account.

In the case of the CCPA, if a company has a footprint far beyond California, they can consider creating a bespoke California web experience to remain compliant. But many companies have taken a cue from California and implemented a *Do Not Sell* option across all regions to ensure privacy best practice.

Set a Process for Handling *Do Not Sell* Requests

A *Do Not Sell* button is only the first step needed to respect the CCPA provision. When a request comes in, your team needs to be able to find and remove records from relevant data locations. In a company with large volumes of data and data requests, the ongoing maintenance of consent preference management can quickly grow burdensome.

Furthermore, the possibility for human error is high, and failing to honor the consent preferences of a user can expose a company to financial penalties under CCPA law. Even if you chose not to implement an automated solution for consent management, it should never be done in an ad-hoc manner.

Check The Administrative Boxes

Last, it's time to review policies and relationships throughout the business.

Review & Update Your Privacy Policy

Turn attention to your privacy policy. Privacy policies are the most important document a business has for articulating the way it cares for user data. According to contemporary best practice, privacy policies should be clear, lucid documents free from "legalese" as much as possible.

To comply with CCPA, GDPR, or most other modern privacy laws, you'll need to update your policy to include the *what*, *why*, and *how* of all personal data your business collects, and the rights that your customers have regarding the collection, storage, and processing of their data. CCPA-compliant businesses must also include a *Do Not Sell* link in their privacy policy.

Review Your Relationships with Third-Party Vendors

A final important step for getting your business on the right privacy track. It's not just about auditing your partners to make sure they don't pose a privacy risk to your customers—it's about understanding how your relationship is classified under CCPA, and what obligations result.

The most important vendor distinction in the CCPA is between *third parties* and *service providers*. There are significantly different requirements for how a business deals with each, from data disclosure to the processing of consumer requests. Thus, classifying each vendor is vital.

Train, Train, Train Your Team

No privacy operation, not even one using Ethyca, can run smoothly without team buy-in. The more educated your team is on the importance of doing privacy right (and the consequences of doing it wrong), the better the outcome will be for your business.

Consider appointing a Data Protection Officer to oversee privacy education for your team. Because even if a business takes all the steps above to safeguard their data operation, a single uninformed employee can put the business at needless risk if they don't follow basic privacy practices. An empowered DPO can train the team to avoid those mistakes.