

PRIVACY RESOURCE PACK

REDCL**VER**
ADVISORS

REDCLOVERADVISORS.COM

**CCPA IS NOW
ENFORCED, WHAT
DOES MY COMPANY
NEED TO DO?**



The California Consumer Privacy Act (CCPA) has been on the horizon for a long time. It was passed on June 28, 2018, but the lead time on finalization and enforcement has been a slow road.

However, the wait is over – enforcement has become enforceable as of 2020. (Yes, it's been in effect since January 1, 2020, but it's the real deal now, complete with final rules and all.)

A lot has changed since CCPA first rolled out. And a lot has REALLY changed since January. So what's a privacy-minded organization to do if they need to get up to speed on falling in line with CCPA regulations?

WHAT'S IN CCPA (AND WHAT'S IN IT FOR ME?)

It's never a bad idea to start with a refresher on what exactly is going on with privacy regulations. By necessity, privacy regulations are complex and nuanced. CCPA is no exception.

CCPA is the most expansive data privacy law to date in the United States. Informed by advertisers using consumer data without consent to influence events like political elections, it's regulatory reach goes beyond the borders of California.

CCPA is often said to be the lite version of GDPR. That's not inaccurate, but there are some important differences to make note of now that we're entering into the enforcement period of CCPA.

DOES CCPA APPLY TO ME?

Anytime there is a new regulation, the first question that pops into a business owner's head is, "Okay, do I need to worry about this?"

So, if you're in a compliance state-of-mind and thinking you should probably dig into whether or not you need to start scrambling, here's the short answer for you. Utilize the checklist below to determine if CCPA applies to you:

Do you do business in California?

Yes No

Is your business located in California?

Yes No

Do you do business with California residents?

Yes No

Is your business collecting information from California residents?

Yes No

Are you a for-profit business?

Yes No

IF YOU ANSWERED YES TO ANY OF THE ABOVE QUESTIONS, THEN THE CCPA MIGHT APPLY TO YOUR ORGANIZATION. HOWEVER, YOUR ORGANIZATION MUST ALSO FALL WITHIN ONE OF THE FOLLOWING:

- It must have an annual gross revenue of more than \$25 million.
- It must annually buy, receive, sell, or share the personal information of more than 50,000 consumers, households, or devices for commercial purposes.
- It must derive 50% or more of its annual revenue from selling consumers' personal information.

IF YOU HAVE CHECKED THE BOX NEXT TO ONE OR MORE OF THESE CONDITIONS ABOVE, THEN CCPA APPLIES TO YOUR ORGANIZATION. THE CHECKLIST BELOW IS A GREAT FOUNDATION TO ENSURING YOUR ORGANIZATION'S COMPLIANCE WITH THE CCPA.

- Conduct an evaluation of the data that your business is collecting from California residents **(including where you're collecting data from, how you are processing the data, and who has access to this data - including 3rd parties)**
- Develop a data inventory of all personal information collected, processed, or sold from California residents
- Create a "Do Not Sell My Personal Data" button on your business's homepage with a clear explanation of the consumer's rights under the CCPA
- Create a documented consumer request process that verifies each customer before responding to their requests **(your customers have the right to request to opt-out, to receive access to their data, and to deletion)**
- Ensure that your business is providing equal rights and services to your customers **(your business shouldn't be changing prices or rates per customer nor providing different levels of quality to customers exercising their rights under the CCPA)**
- Provide your employees with training
- Implement proper cybersecurity safeguards and frameworks in order to protect your business & customers' personal information from unauthorized breaches
- Obtain consent for children under the age of 16 before selling their information (children 0-13 need parental consent, children 13-16 can consent directly)
- Maintain an incident response plan and method of notification if there is a data breach of customer information

If you have any questions regarding what the new CCPA law means for your business, let's talk. **Click here** to schedule your FREE Privacy Risk Assessment to discover how Red Clover Advisors can help your business stay compliant with CCPA and protect your customers.

RED CLOVER
ADVISORS

 www.redcloveradvisors.com |  info@redcloveradvisors.com

DISCLAIMER: The materials available in this document are for informational purposes only and not for the purpose of providing legal advice. Red Clover Advisors, LLC is not a law firm, and if you need legal advice, please contact a competent attorney to provide appropriate legal advice with respect to your specific concern.



**GDPR AND
YOUR BUSINESS:
WHAT DO YOU
NEED TO DO?**

REDCL**VER**
ADVISORS

The General Data Protection Regulation (GDPR) addresses the transfer of personal data outside the European Union (EU) and the European Economic Area (EEA). It gives control to individuals over their personal data and addresses the transfer of personal data outside the EU and EEA areas. It came into effect in May of 2018 and it affects any company that conducts business with customers in the EU.

WHAT IS GDPR?

In short, GDPR has to do with any company that collects the personal data of their customers in the EU and EEA, whether their business physically resides there or not. Your business must disclose (clearly) any data collection, declare the purpose for data processing, and disclose exactly how long the data is being retained and if it is being shared with any 3rd parties. Companies are being fined millions of euros if they aren't in compliance.

DOES GDPR APPLY TO ME?

Is your business located in the European Union OR does your organization conduct business with consumers who are located in the EU?

Yes No

If your business is located outside of the EU, are you selling goods or services to consumers within the EU?

Yes No

Is your business processing data of your consumers within the EU?

Yes No

Does your business have data controllers and/or processors that are established in the EU?

Yes No

Are you monitoring the behavior of European residents?

Yes No

IF YOU HAVE REPLIED YES NEXT TO ANY OF THE ABOVE QUESTIONS, THEN GDPR APPLIES TO YOUR ORGANIZATION. THE FOLLOWING CHECKLIST IS A GREAT FOUNDATION TO ENSURING YOUR ORGANIZATION'S COMPLIANCE WITH THE GDPR.

- Conduct an evaluation of the data that your business is collecting from California residents **(including where you're collecting data from, how you are processing the data, and who has access to this data - including 3rd parties)**
- Determine the legal justification for your data processing
- Determine what cookies you are using on your site such as for advertising, analytics, user login, or fraud, and create a cookie banner to collect consent.
- Determine whether or not you are collecting data from individuals less than 16 years old (if you are, you must obtain parental consent and ensure your privacy notice is age-appropriate)
- Identify if your business is using personal data for research
- Create a process for handling deletion requests
- Create a process that allows consumers to correct their personal information
- Create a process for customers to request that you stop processing their data
- Create a process for customers to easily request a copy of their personal information
- Create a process notifying the correct authorities and data subjects in case of a data breach
- Integrate data protection into your entire product development process and into all data processing
- Appoint an individual who is responsible for ensuring your organization's compliance with the GDPR
- Conduct a Privacy Impact Assessment to identify the type of personal information you are processing and evaluate the risks of collecting such data

If you have any questions at all regarding what the new GDPR law means for your business, let's talk. **Click here** to schedule your FREE Privacy Risk Assessment to discover how Red Clover Advisors can help your business stay compliant with GDPR and protect your customers.

RED CLOVER
ADVISORS

 www.redcloveradvisors.com |  info@redcloveradvisors.com

DISCLAIMER: The materials available in this document are for informational purposes only and not for the purpose of providing legal advice. Red Clover Advisors, LLC is not a law firm, and if you need legal advice, please contact a competent attorney to provide appropriate legal advice with respect to your specific concern.



INCREASING CUSTOMER ENGAGEMENT IN A WORLD OF PRIVACY REGULATIONS



PRIVACY LANDSCAPE

Today's privacy landscape makes it difficult for marketers to develop and maintain relationships with customers/prospects in traditional ways. It seems that for most interactions, user consent is needed. It may be opt-in or opt-out, but the fact remains the same – the customer engagement landscape is changing, and marketers need permission to contact users and build relationships. So how do we, as marketers ensure that users are willing and even eager to provide us the important details that marketers need to effectively do their jobs?



[Schedule Your FREE Privacy Risk Assessment](#)

THE ANSWER IS SIMPLE...



MAKE THE USERS WANT TO INTERACT WITH YOU.

But the delivery of that is less clear. Below we have provided several tips on how to achieve this goal:

HOW TO ASK FOR CONSENT



IT'S ALL IN THE ASK

In many cases, especially for marketing activities, consumers need to consent to having data being collected on them, but did you know that “how” you ask for consent can determine how much data users are willing to share? When your company asks for consent, it should be on brand - the tone of the documents or cookie banners as well as the design of them (some [JD1] call this Privacy UX). Different geographies have specific rules on how these consent banners need to operate and what is said, but the overall tone and content can be customized within that to reflect your brand. When this happens the user feels comfortable

BE CLEAR + TRANSPARENT

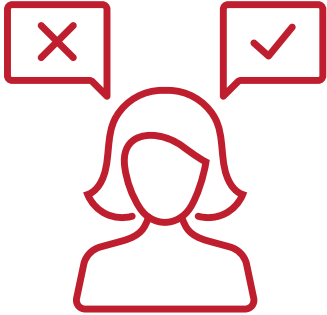


It is of utmost importance to be transparent about what you are collecting and why is important, as is writing it in a clear and easy to understand language. Whether it is asking for consent, providing a privacy statement or explaining what cookies are being collected, it should be clear and written in easy to understand language – not legalese. This transparency helps build trust with the user and will increase their comfort level in providing data to you.

PROVIDE BENEFITS

It is also important for the user to understand “what’s in it for them”. In other words, why do they benefit by providing personal information. Will they get more customized offers, will they only see the product they want to see? In a Deloitte study, 79% of consumers said they would be more willing to share personal data if there was a clear benefit to them. Harvard Business Review tells us that customers have a fear of missing out, so let them know exactly what they will be missing out on!

GIVE USERS CHOICE + CONTROL



**WHEN CHOOSING THE WHAT/WHEN/WHERE
ABOUT PROVIDING PERSONAL INFORMATION,
MAKE SURE THE USER HAS CHOICE AND CONTROL
- AND THAT IT'S EASY TO FIND.**

THE PROOF IS IN THE PUDDING

DID YOU KNOW?

According to a recent Emarketer Study, 69% of Internet users want control of email frequency and 63% want control over email content but on average, only 10% and 24% of retailers offer this, respectively. So there's plenty of room for improvement. When consumers sign up for product emails, let them choose to get information on clothing sales, but choose not to get email/offers related to furniture. Or if you are an online news publisher, give consumers the opportunity to get updates daily, weekly, or just if there's breaking news. If at any time they want to change these preferences, make it easy to find - possibly in the global footer or a visible link in an email.

**KNOWING THEY CAN CHANGE THE SCOPE OF THE
RELATIONSHIP AT ANY TIME WILL HELP TO BUILD TRUST WITH
THE CUSTOMER.**

[Schedule Your FREE Privacy Risk Assessment](#)

PERSONALIZATION



AS MARKETERS WE KNOW THE IMPORTANCE OF PERSONALIZING A USER'S EXPERIENCE. HOWEVER, IN MANY SITUATIONS WE ARE PROVIDING PERSONALIZED EXPERIENCES THE CONSUMER MAY OR MAY NOT WANT.

USING 1ST PARTY DATA

Just because a consumer looked at a pair of shoes online does not necessarily mean he/she wants ads of those shoes following them all over the Internet. We are using first, second and perhaps third-party data to anticipate wants and needs. But we aren't asking directly. Ask your customer what types of products they want to get information on, and then use that first party data to provide updates on sales, offers, etc. If you focus your personalization efforts using just information that they actively gave you, they will feel more comfortable continuing to provide that information and trust that you have their best interests in mind.

While privacy regulations may initially appear challenging for marketers, it is clear they are here to stay. But it is also clear that there are ways to work in this new environment to build trust with your customers and possibly have an even stronger relationship by taking some of the approaches mentioned above.



RED CLOVER ADVISORS

Thank You!

**Schedule Your FREE
Privacy Risk Assessment**

DISCLAIMER:

The materials available in this document are for informational purposes only and not for the purpose of providing legal advice. Red Clover Advisors, LLC is not a law firm, and if you need legal advice, please contact a competent attorney to provide appropriate legal advice with respect to your specific concern.

Schedule Your FREE Privacy Risk Assessment