REDCLOVER ADVISORS

6 Steps to Privacy Compliance for Marketers

www.redcloveradvisors.com | info@redcloveradvisors.com

REDCLOVER ADVISORS

6 Steps to Privacy Compliance for Marketers

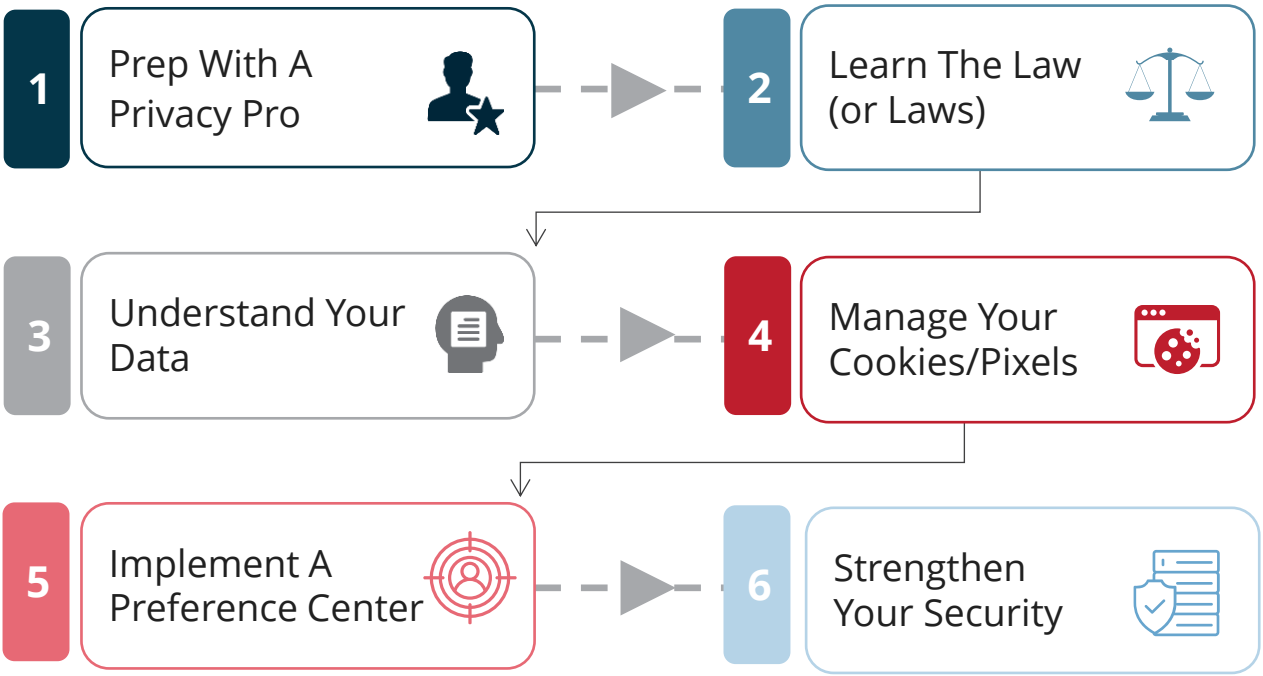
Primer

Marketing professionals love a good creative brief, brand statement, email flowchart, or detailed content calendar. But what about a good privacy regulation?

Well, where in the world do you even begin? Do you need to follow GDPR, CAN-SPAM, or the other nearly 20 state privacy laws? How do you even understand what they're asking you to do—and how they're asking you to do it—when it's hard enough to keep the names and acronyms straight?

Most company-collected consumer data is used for marketing purposes. And because marketing processes need to align with legal requirements and privacy best practices – it is critical for companies to have a privacy strategy as business processes or regulations change.

6 Steps for Marketers



1 PREP WITH A PRIVACY PRO

There are a lot of off-the-shelf programs that promise total compliance. But the reality is that most of these programs will fall short without help from a privacy expert who understands the nuances of your company's specific use cases and any applicable privacy regulations.

Whether you have an established privacy program or are just starting to dive into data privacy, utilizing a privacy consultant will save you time and money in the long run by ensuring you stay on the right track.

2 LEARN THE LAW (OR LAWS)

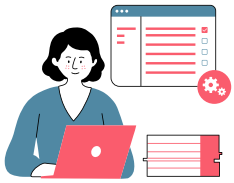
Companies that operate in or collect data from residents of the European Union are subject to the grandfather of all data privacy laws, the General Data Protection Regulation (GDPR).

The GDPR establishes strict consumer consent guidelines, as well as rules regarding data collection, use, and storage, consumer rights to privacy, and penalties for non-compliance.

Internationally, GDPR has been a lynchpin in privacy regulations, but it's not the only game in town. Canada, Brazil, China, and other major global powerhouses have—or are working on—similar legislation that is important for marketers to understand.

In contrast, the United States doesn't currently have a federal data privacy law, but that doesn't mean U.S. companies are exempt from privacy regulations. 19 states have passed laws (as of Q3 2024) protecting their residents, and many more have legislation in the works. Depending on your company's size, industry, and client base, your company may be subject to more than one privacy law.

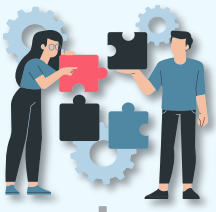
3 UNDERSTAND YOUR DATA



Most companies don't fully understand their data because they collect more data than they need, share it with too many people, and hang on to it for too long. Having only a partial understanding of your data means that your company has accepted a significant amount of unnecessary risk, whether you meant to or not. It's time to take a closer look at how data flows through your company.

6 STEPS TO UNDERSTAND YOUR DATA

1 Complete a Data Inventory



A data inventory, sometimes called a data map, can give your organization insight into what types of data are being collected and why, who has access to it, and where (and how long) it's being stored. Marketers typically collect data that includes name, email, and phone number. Sometimes marketers collect other information that consumers may question or not want to provide, like income, personal preferences, health conditions, or concerns.

Performing a data inventory is critical to learning where risks and vulnerabilities are. Get started by downloading our data inventory template and resource guide.

2 Understand Do Not Sell/Do Not Share

Most privacy laws, while they don't explicitly say it, often regard AdTech activities, including targeted advertising and analytics, as a "sale of data." Some jurisdictions even require organizations to provide individuals the option to opt out of targeted advertising.

And under CCPA, businesses are required to include a link that says, "Do Not Sell/Do Not Share My Personal Information" on a website's homepage with a link in the footer, or by using the CCPA icon that states, "Your Privacy Choices."

3 Review Your Privacy Notice

Many companies have a privacy notice that's a holdover from the early days of the internet—complete with pages of dense, legal terminology describing outdated data privacy practices. A marketing-friendly privacy notice (download our Privacy Notice guide for more info) uses plain language to clearly explain data that your company collects, uses, stores, and shares.

6 STEPS TO UNDERSTAND YOUR DATA

4 Optimize Opt-In & Opt-Out Processes

Most U.S. data privacy laws mandate that consumers can opt out of having their data collected or processed (think the little box under an email submission form that says 'I consent to receive advertisements and other marketing communications from XYZ company and its partners').

Adopting a consumer opt-in approach is even better than providing opt-out opportunities because it gives consumers the most control over their personal data. Keep in mind that some privacy regulations—like GDPR—have specific consent standards that you need to follow, such as not pre-ticking boxes when the user opts in. Proceed accordingly.

TAKE NOTE!

Laws differ by region when it comes to email marketing consent requirements. Consider where you're located, where your customers are located, and what you need to know about CAN-SPAM, CASL, GDPR, or other applicable requirements.

Create a Process for Privacy Rights Requests 5

Most privacy laws require businesses to establish processes that allow customers to correct or delete their information from company databases. Managing these requests demands legal and operational expertise (learn more by downloading our Privacy Rights Guide here). To maintain compliance, it's important to establish an efficient workflow for processing these requests.

6 Conduct Privacy Impact Assessments (PIAs/DPIAs)

A privacy impact assessment (PIA) is a complex task that involves evaluating the risks to personal information associated with an organization's processes, services, or products. Its primary legal purpose is to ensure compliance with many data privacy regulations. Targeted advertising is a common marketing activity that requires a PIA. Download our Privacy Risk Assessment Guide for more information on the PIA process.

4 MANAGE YOUR COOKIES

Most privacy and data protection laws require cookie management, whether that means obtaining consent or otherwise (see our Cookie Management Guide here). And thanks to the changing landscape of privacy laws and consumer preferences, managing your use of third-party cookies and other tracking technologies requires continuous diligence and adaptation.

Create Long-Lasting Compliance

(applies to cookies and other types of pixels and tags)

EXAMINE THE PURPOSE OF YOUR COOKIES

Assess what information your cookies collect and what their purposes are. Know what laws apply to you and your notice and choice obligations around cookies, targeted ads, and profiling.

IDENTIFY AND CATEGORIZE COOKIES

Identify and categorize all existing cookies and separate them by type. Use cookie consent software to automate this process.

BUILD AND IMPLEMENT A COOKIE CONSENT BANNER

Depending on your business and the jurisdictions you fall under, you may need to add a cookie banner or other consent solution to your website to provide requisite notices and enable users to opt-out (or opt-in) per applicable privacy laws.

RECOGNIZE UNIVERSAL OPT-OUT MECHANISMS (UOOMs)

UOOMs, like Global Privacy Control (GPC), are browser settings that notify websites of a user's privacy preferences. These signals must be recognized, allowing individuals to opt out of the sale or sharing of their personal information for targeted advertising.

TEST THE TECH

Ensure the consent and opt-out mechanisms you provide are effective, sufficient, and in working order. Does your cookie banner work as it should? Are cookies properly firing? Does your system block cookies if a consumer hits "reject cookies"?

REVIEW NOTICES

Make sure your privacy notice and/or cookie notice is up to date and accurately describes the cookies you use and the choices you provide to users.

CREATE A COOKIE GOVERNANCE PROGRAM

A broader program to review all the above on an ongoing basis and determining what cookies/pixels should be there in the first place.

Clean Up Your Cookie Banner

In Europe and elsewhere around the world, consent is required for the use of nonessential cookies, think tracking or analytics cookies, and in many U.S. states, residents now have the right to opt out of cookies that are used in the sale or sharing of personal information as well as targeted advertising. The most common way companies manage this notice and choice obligation is with a cookie banner.

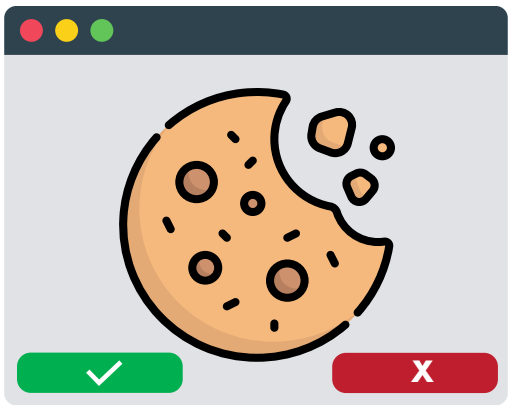
Even if it isn't strictly required, cookie banners can increase the trust between you and your customer by creating transparency surrounding your data collection practices.

Cookie Banner Best Practices

Depending on the laws applicable to your company, you will need to provide notice of the types of cookies included on your site and the consent options available to the user.

When building or revising a cookie banner, it needs to make sense and should:

- ✓ Be visible, easy to understand, and accurate
- ✓ List the types of cookies used on your website
- ✓ Include proper language that describes the purpose of each cookie
- ✓ Include options for users to exercise rights, giving equal choice between accept and reject
- ✓ Ability to manage the cookie settings from the cookie banner
- ✓ Be formatted without "dark patterns," e.g., font/color/box shape discrepancies that push the consumer to "accept" rather than "reject" cookies
- ✓ Link to your privacy notice



If you use third-party cookies, check your company's website cookie consent mechanisms to ensure they're firing at the right time and provide the correct consent notice, enabling users to affect choice, whether opt-in or opt-out.

Once you have a cookie program in place, it's important to test and iterate regularly (we recommend at least twice a year) to make sure things are working as you intended.

5 IMPLEMENT A PREFERENCE CENTER AND/OR TRUST CENTER

Everyone likes to have choices. This is especially true when you're talking about giving your customers options for how they want you to handle their data—and it can be as easy as building a preference center.

A preference center is often a component of first-party data programs. It's a page on your website or app where users can tell you how you may use or share their personal information. As a privacy tool, preference centers have multiple benefits for your businesses. For one, they give your customers the chance to tell you:

- The type of emails they want to receive
- Their interest in receiving text messages
- How often they want to hear from you
- The topics they want you to contact them about (new products, webinars, events, etc.)
- Their preferred communication channels (text and/or email)
- The volume of content they'd like to receive, from all marketing communications to nothing at all

Benefits of a Preference Center

MAKES MARKETING MORE EFFECTIVE

They simplify data management by allowing customers to update their information and indicate when and how you may contact them, how often, and about what.

GIVES YOUR MARKETING A COMPETITIVE EDGE:

Customers pay attention to how you handle their information. Having a preference center demonstrates that you take your customers' preferences—and privacy—seriously.

THIS HELPS YOU:

- Increase your open rates
- Retain subscribers with customizable communication options
- Maintain up-to-date data sets for your clients—with minimal extra effort
- Build better ROI by targeting your ideal audiences for services, products, and information
- Help you establish compliant opt-out/opt-in and DSAR processes
- Reduce unsubscribes, blocks, and email deliverability issues

Take the Extra Step: Building Trust Centers, Builds Trust

Trust centers are the natural next step of privacy centers, allowing you to centralize all your privacy-related information, activities, and services (including preference centers). Make it visually engaging and infuse your brand's voice on this page.

6 STRENGTHEN YOUR SECURITY

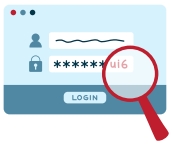
Cybersecurity and data privacy aren't the same thing, but they are connected.

Even the best cybersecurity program will only succeed if the right privacy practices are in place. On the other hand, a privacy program that ensures responsible and ethical use of data can't match a firewall's effectiveness at stopping an external breach. Beefing up redundancies in both areas will reduce the risk of exposure.

Addressing Human Error in Data Breaches

Did you know that 74% of data breaches are caused by human error? Implementing updated standard operating procedures for tasks like installing software updates, patches, and license renewals can help minimize hacks resulting from oversight. The same rule applies to network and database usage: restricting employee access to only necessary information needed to complete a task adds an extra layer of security around valuable and sensitive consumer data.

Marketing Teams Can Manage Security With:



Strong Passwords

+

Multi-Factor Authorization on Every Tool Possible

+

A Password Management Tool to Store & Share Passwords

Importance of Privacy-Minded Vendors

In today's interconnected business landscape, most marketing agencies rely on external vendors and service providers to fulfill their duties. Most data privacy laws hold companies accountable for data exposure even if a breach occurred due to vendor error, so it's crucial to vet your vendors privacy practices. Take stock of your vendors privacy practices, what you share with them, and adjust as needed. Vendors with non-compliant or subpar data management practices should be replaced with more reliable partners.

Training is Critical

Continued employee education is essential to building a culture of privacy that will take your company beyond compliance and into thought leadership. Even a five-minute weekly staff meeting refresher will keep privacy top of mind for your marketing and customer service teams.

DATA PRIVACY IS HERE TO STAY!

As you've seen throughout this guide, privacy compliance is not just a legal obligation—it's a critical component of building and maintaining trust with your customers. By embracing privacy, you're not just avoiding risks—you're creating a foundation that strengthens your relationships with customers and sets your business up for long-term success.

This is something every marketer should be proud to stand behind!

This marketing guide serves as an excellent starting point. And if you need more help, the privacy experts at Red Clover Advisors are ready to assist. We have the knowledge you need to create and implement compliant, consumer-focused data privacy programs no matter where you are on your privacy journey.

Schedule a consultation with our privacy pros today and see the difference experience makes.

WONDERING HOW YOU CAN GET IT ALL DONE?

WE CAN HELP

Our team of privacy experts can help navigate you through best practices, strategies, and tactics. Contact us for a consultation.

www.redcloveradvisors.com