



# ACHIEVING **TRUST** THROUGH **COMPLIANCE**

A MARKETER'S GUIDE TO CUSTOMER DATA PRIVACY



# A MARKETER'S GUIDE TO CUSTOMER DATA PRIVACY

As a marketing professional, how can building a strong privacy compliance foundation help your organization build trust and improve the Customer Experience? What do you need to know, how and why should you seize this moment?

2020 marked an important milestone for marketing professionals when enforcement started for the California Consumer Privacy Act (CCPA) comes into force. It's the latest legislation in a creeping trend of increasing regulation over data privacy compliance both nationally and internationally.

Far from being a grudging obligation, you should view this as a golden opportunity to reinforce the very foundation of Customer Experience for your brand: Trust. By merely throwing money at compliance, you miss the chance to double-down on this critical aspect of Customer Experience (CX). After all, trust builds loyalty; loyalty leads to higher customer lifetime value and, therefore, your bottom line.

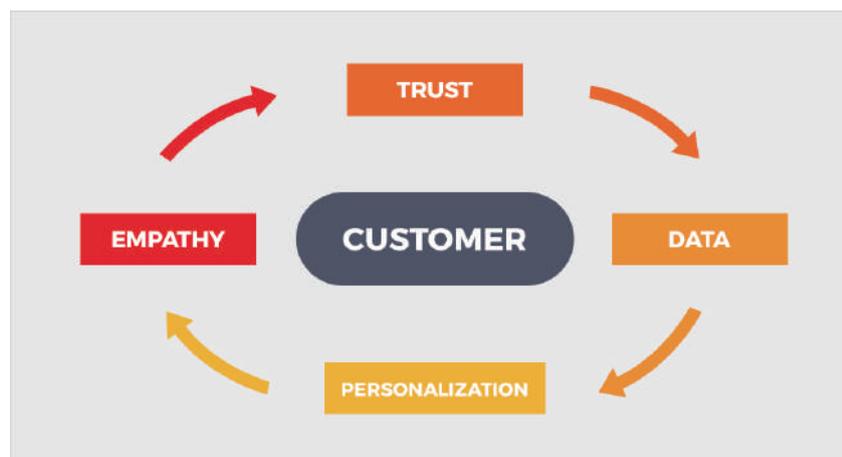
As a marketer, you should grab every opportunity that comes your way to invest in the customer experience. Don't waste your precious dollars on a quick compliance patch-up job!

# Why TRUST?

When it comes to CX, trust is everything.

Long ago, you may recall reading about Abraham Maslow's [Hierarchy of Needs](#) as a psychological theory to explain human motivation. It describes how basic 'physiological' and 'safety' needs are at the bottom of the pyramid – the foundation stones. These are essential before seeking higher-level needs like 'belonging' and 'esteem.' You can apply the same basic principles to your customers when it comes to their critical needs from your brand.

The research and advisory firm, Gartner, almost got it right when they created their [CX Pyramid](#) as a framework for designing powerful experiences. But today, with privacy compliance at the forefront of many marketing investments, it should be expanded to include a more fundamental foundation layer for customers: "Provide an Experience I can Trust." In today's political and consumer environment, if you omit this essential element, other aspects of the experience will be flawed.



When you think about it, data compliance is a fundamental, essential component of trust. Without trust, your customers will be reluctant to share their precious personal information. Without it, you can't focus on personalization, building rapport, and empathy. These are the elements that build deeper trust. And it's a virtuous circle.

Privacy Compliance might sound like a dry and academic concept, but when you view this through the lens of creating and maintaining trust, it takes on a whole new level of importance.

This guide explains the essential relationship between compliance, trust, and customer experience. We take a closer look at the privacy compliance requirements, why you should care, and crucially, how to respond by placing **trust** front and center of your CX strategy.

Let's start with the basics.

Nearly half **49%**

of marketers believe consumers' trust in how brands handle their data has improved since GDPR came into force in 2018. A further 46% say that trust in brands has improved too.

Source: DMA

## What is Privacy Compliance?



For over a decade, digital marketing optimized how it communicates with customers, working very hard to reach them exactly how and where they would like to receive communication. This ensured the best possible result. Today, we have more channel choices than ever – contact centers, social media, email, and smartphone apps. We have long had the technology for customers to express their communication choices and preferences. You would think there should be nothing new required to be compliant. However, the answer is more complicated.

To illustrate, let's start with what are currently some of the strictest obligations for privacy compliance and contrast them with other less stringent rules.

For many, privacy compliance may be a legal obligation to keep your customers' data secure and follow specific guidelines when handling personal information. Also, it concerns transparency and acting in the best interest of the people whose information you collect.

Laws may also require that customers give explicit, informed consent to retain their data, and they must be able to rescind this permission at any time easily. In the case of GDPR, customers also have the right to be forgotten and retrieve or transfer their data to another organization.

However, another jurisdiction might not require explicit consent for storing customer data but may need to present an option to opt-out of selling their data.

In the EU, if consumers refuse to grant permission to use their data, you can't penalize them by delivering a lower level of service or higher prices. However, this may not be the case in other countries.

And that's not all. Not only does your organization need to be compliant, but you need to prove it. It must be tracked assiduously and be auditable – keeping what we call a “legal archive.” If an individual or a regulatory agency claims you are in violation, your best defense is clear evidence that you provided the required disclosures and received permission to collect or use a customer's

Also, it bears reminding that you should not assume that you can throw the same business rules at GDPR, CCPA, and all the other legislation in the pipeline. (For example, Nevada's [Senate Bill 220](#) (SB 220) diverges significantly from CCPA in several ways.) Each has its nuances, and we will likely see most legislation amended over time. In other words, **privacy compliance is a fluid situation, not a one-and-done exercise.** You need to plan carefully and build in the flexibility you will need for the future.

#### **How does CCPA compare to GDPR?**

The industry group, Future of Privacy Forum recently published a [useful side-by-side comparison](#) of the similarities and differences.

Source: FPF.org

And finally, if you plan to build trust through compliance, then you must understand both the letter and the spirit of these laws and regulations. A best practice is taking into consideration your company's policies and culture and use them as discussion points. They are invaluable when planning improvements to the customer experience and achieving trust through compliance.

# Where and When does it apply?

The most widely recognized compliance legislation was introduced in 2018 by the European Union – [GDPR](#) – the General Data Protection Regulation, which came into force on 25th May 2018. But it's worth noting that [Canada's Anti-Spamming Legislation \(CASL\)](#) dates back to 2014.

The next relevant legislation is the [California Consumer Privacy Act \(CCPA\)](#), which came into force on January 1st, 2020. As the fifth-largest economy in the world, it makes sense they would be one of the first. Additional states have [similar legislation](#) under consideration. Near the end of 2019, we started to see increased discussion about US [federal privacy compliance proposals](#) in the media.

The bottom line is that privacy compliance legislation is becoming more pervasive and restrictive, not less.

# To Whom does it apply?

Privacy compliance legislation applies to not only companies operating in each jurisdiction, but also ANY company sending commercial communications, collecting or processing data to consumers residing there.

It may also apply to so-called 'data brokers'; companies with no direct relationship with the consumer but who store, process, or sell customer data.

There are a few exemptions for small businesses and not-for-profit, charitable organizations, but otherwise, you need to be 100% compliant.

In short, if you're a company of a reasonable size and you think that it might apply to you, you're almost certainly right. So, all marketing professionals need to take urgent steps to ensure you're compliant. But more importantly, taking concrete steps to achieve compliance also provide a better foundation for building trust.

But if you're intent on building lasting trust and loyalty with your customers, the bar may still be set too low. Your aim is to build trust your customers expect from you, while also meeting your privacy compliance obligations. A high bar also makes it more difficult for your competitors and can help build the trust your customer will appreciate.

# Why now and Why should you care?

Putting it bluntly, privacy advocates and legislators around the world have lost patience with the lack of self-regulation by technology companies and have decided to step in. Data and privacy protection laws have fallen very far behind today's information-rich, tech-fuelled consumer landscape. They've decided to tighten up the rules, put the consumer first and in control of their data, and come down hard financially on those who continue to flout them.

## Carrot and Stick

Let's start by getting the 'stick' out of the way. GDPR violations can attract fines of up to EUR 20 million (or 4% of global turnover, whichever is greater). CCPA, on the other hand, has a maximum civil penalty of \$7,500, but this is per violation. So, if you mishandled just 100 customer records, the penalties rack up very quickly. (CCPA also entitles individual consumers to compensation up to \$750 in addition to the civil penalty!)

That's the bad news. Your marketing 'best practice' should be about building a foundation of trust to deliver a superior customer experience. Then, shouldn't regulations be the 'low watermark' for your treatment of customer data? If you're seeking lasting customer loyalty to maximize their lifetime value, shouldn't your aspirations set the bar higher?

By putting the customer in control of their data, contact, and content preferences, you can achieve the CX 'El Dorado' of hyper-personalization. There is a direct link between trust and customer lifetime value (CLV). A 5% improvement in customer retention can have a 25-95% impact on business profits [The Economics of E-Loyalty](#), Harvard Business School. Organizations that embrace privacy compliance will reap enormous benefits in trust, loyalty and customer retention.

### THE CUSTOMER IN CONTROL

Subscription Management is a key strategy for organisations putting their customers in more control of their own data and how it's used. To find out more, [download our free whitepaper](#).

Source : 4Thought Marketing

So, now you have the basics of privacy compliance, and why it's critically important for your brand, the big question is...how will you respond?

# How should you respond?

Of course, you could make some ad hoc changes to your existing systems, patch them up, and push them out there. And this may be your current, budget-friendly plan. The problem with this approach is that it's a time bomb. At the very least, the cost of ownership of your marketing automation solutions will grow and grow as each new slice of legislation requires more and more detailed changes. But in the worst-case scenario, and more importantly, you could lose a massive opportunity to create deeper trust with your customers.

## Future-Proofing Your Privacy Compliance

The smart approach to privacy compliance is to build a flexible framework. It will help reduce future effort, lower the total cost of ownership (TCO), and focus on delivering personalized, timely, and relevant communications to your customers. The benefits of a little more upfront planning and investment will far outweigh the burden of implementing future changes to legislation both nationally and internationally.

## Seize the Opportunity

Work collaboratively with digital marketing, improve customer websites, make trust, and “the customer is in control of their data” your mantra...

For Marketing professionals, there's a simple answer. 4Thought Marketing offers a [compliance API solution](#) that takes the hard work out of building this capability from scratch. Our compliance solution covers the full Privacy Compliance lifecycle from data upload, form compliance (for landing pages), customer Rights Management (including the right to access, update and porting data, as well as the right to be forgotten), and compliance reporting. The whole process is made more manageable through our dashboard. So, in the future, you can accommodate critical changes to legislation through simple administration and not expensive coding changes. Additionally, our [Privacy Compliance experts](#) are on hand to ensure a smooth transition and answer your marketer's questions.

Any framework you choose to implement must offer you the flexibility to deploy jurisdiction-specific functionality for specific customer segments (rather than a ‘lowest common denominator’ approach, applying the most restrictive legislation to all customers.)

Another key reason for deploying a compliance-ready framework is that it respects the many nuances between legislation like the right for customers to download or move their data to different companies. This right will differ depending on which legislative territory where your customer resides. In the United States, several big companies are [lobbying for federal legislation](#) to unify Privacy Compliance; however, this is unlikely to happen any time soon. State-specific laws are already underway.

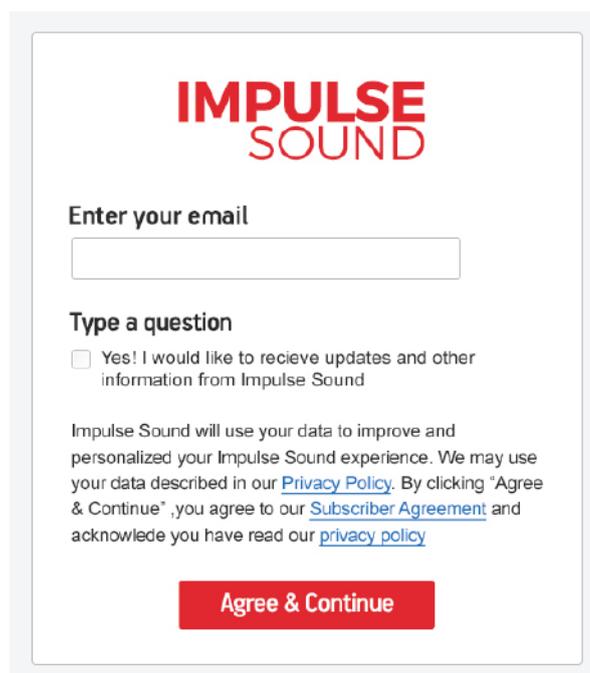
## From Compliance to Trust

Once you’ve implemented the basic framework, you can then look at those trust-building components where you pass control to your customers, so they have the choice to configure their own experience (if the default offered to them doesn’t suit). We now move into the domain of Subscription Management – closely related to Privacy Compliance – as you allow customers to set their communication and content preferences. Everything from the topic areas of your brand’s content to the frequency of sending it. If you’re interested in learning more about [Subscription Management](#), then [download our recent white paper](#) on the subject.

## Do the Right Thing

As we stated earlier, compliance is not just about asking for explicit consent for storing and using your customers’ data. Just like an email campaign, the request must come at the correct time and for the proper amount of information. Customers should immediately recognize your brand as their friend. Do you know that uncomfortable feeling when an occasional friend or colleague asks for a massive favor beyond your comfort? Like lending them money or giving up your weekend to help them move into a new house or apartment? It’s the same with your brand relationship. When you ask for consent to use your customer’s data or send them content, offer them the choice to make this a one-time consent, or for all similar requests, or decline.

(And they should always be able to revoke these permissions at any time easily!)



The image shows a screenshot of a consent form for Impulse Sound. At the top, the logo 'IMPULSE SOUND' is displayed in red. Below the logo, there is a section titled 'Enter your email' with an empty text input field. Underneath that is a section titled 'Type a question' with a checkbox and the text 'Yes! I would like to receive updates and other information from Impulse Sound'. Below the checkbox, there is a paragraph of text: 'Impulse Sound will use your data to improve and personalized your Impulse Sound experience. We may use your data described in our [Privacy Policy](#). By clicking "Agree & Continue", you agree to our [Subscriber Agreement](#) and acknowledge you have read our [privacy policy](#)'. At the bottom of the form is a red button with the text 'Agree & Continue' in white.

## Mind Your Language

Finally, when you inform a customer of their rights, don't make them feel they need an attorney in the room before they click that box. Too many 'rights management' statements are written in complicated legalese that's impenetrable and, quite frankly, boring. You can be friendly, informal, and still correctly discharge your legal responsibilities. Ask yourself, would your mother, father or grandparents understand it!

Once you've written your "rights management" statement in plain language, don't hide it away in a forgotten corner of your website. Provide a prominent link. Don't forget; it's all part of building trust in your brand. This only works if your policies are in plain view.

## Conclusion

Your organization needs to reframe the need for Privacy Compliance Management as an opportunity instead of a burden. The fact that it is now a legal obligation is a red herring. You should consider it as a critical component for building trust with your customers. And trust is the foundation of all great customer experience strategies. Mastering CX will boost your brand success.

However, your brand needs to deliver the right balance between privacy and personalization. To build trust, you need to get this right every time, never forgetting that every customer has different preferences. Best practice in Privacy Compliance Management, therefore, is a massive weapon in your CX armory. Compliance and trust are two sides of the same coin.

As more and more states and countries around the world implement data protection legislation, make sure you choose a compliance framework built to last. Doing this piecemeal will likely cause you even more problems down the road.

As marketing professionals, we need to embrace the changes and knit compliance into the fabric of our customer experience strategy

### Why Reinvent the Wheel?

4Thought Marketing helps companies review, plan and implement Privacy Compliance solutions.

By combining our Privacy Consulting Services with our 4Comply Privacy Compliance API Solution, we can help you build a foundation for trust in a seamless and flexible way. Why not [contact us](#) to learn more?

# About 4Thought Marketing

4Thought Marketing is a software development and privacy compliance company founded in 2008. We help customers align business and legal objectives, translating them into strategies that produce results. Our services include Marketing Automation and Privacy Compliance Software Implementation, Integration, Customization, Consulting, and Services.