6 Steps to Privacy Law Compliance for Retailers

The dawn of 2020 brought more than winter weather and New Year's resolutions. Retailers must now demonstrate compliance with information privacy laws in the US, such as the California Consumer Privacy Act (CCPA) and, soon, New York's SHIELD law. With strict customer privacy laws, retail information governance to achieve privacy law compliance takes on a key strategic role.

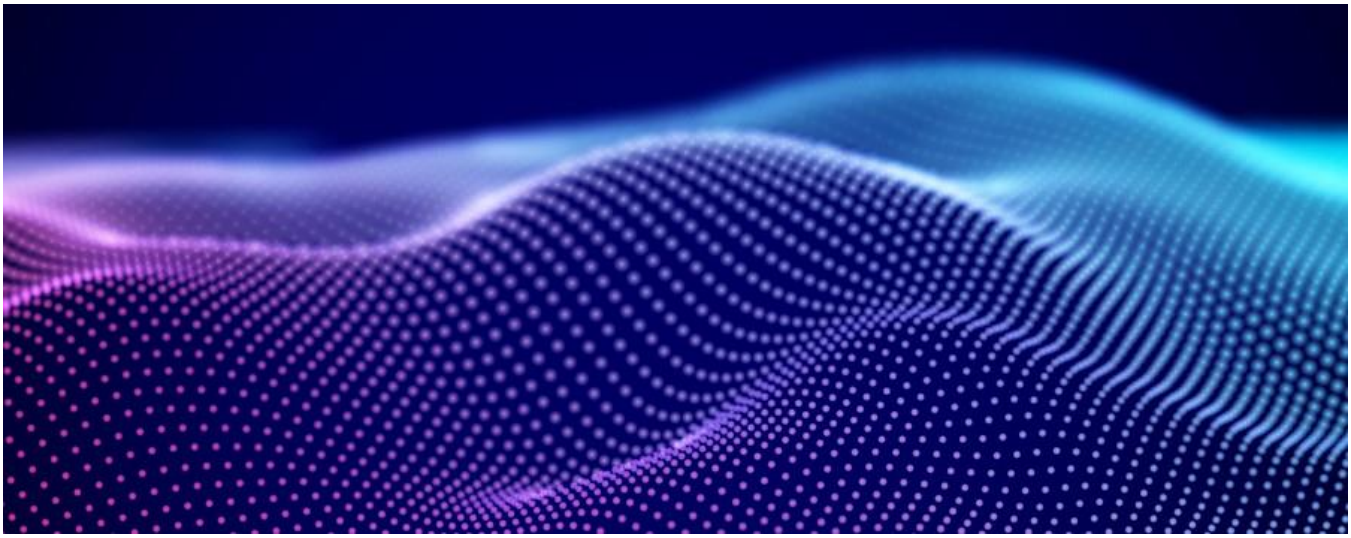
For instance, CCPA mandates that businesses provide consumers control over their private information. That is, consumers can request disclosure of all personal data regarding themselves and their households. They can opt out of the sale of that data, and they can request that businesses delete their personal information.

Like CCPA, New York's SHIELD law expands the definition of private information. It also mandates that businesses implement data security programs to protect against unlawful access to that information. Both laws include strict breach notification requirements and require businesses to address privacy safeguards with third party vendors.

For retailers, laws like CCPA and SHIELD present a significant challenge. Now, more than ever, businesses depend on data to drive marketing and inform strategic decision-making. By implementing the following basic steps to regulatory compliance, businesses can build a privacy culture while harnessing the power of data.

1. Understand Privacy Requirements

The first step to privacy law compliance involves identifying and clarifying the laws that apply to your business. Understand what personal information is protected by the privacy act, as well as the requirements for security programs, breach notification and consumer control of private information.



2. Assess Data Landscape

In order to protect personal information, you have to know where it lives. But discovering all customer data within an organization can prove a formidable challenge. Typically, that data resides in dozens of locations, from marketing to billing, customer support and even third-party vendors.

First, gather key stakeholders. This will include representatives from legal, IT, sales and marketing, HR, finance and other business units. Then, using eDiscovery tools that access multiple platforms, build a data map to show where sensitive data resides, who owns that data and how it flows within the organization.

3. Identify Gaps and Implement a Mitigation Plan

With an understanding of the current data environment and applicable customer privacy law, identify regulatory risks and outline a plan for remediation. Build that remediation into existing privacy programs or use it as the basis for developing a privacy strategy.

For example, you may need to expand data security practices to adhere to SHIELD's program requirements. Or you may need to tag data to facilitate the ability to quickly locate and delete sensitive information in compliance with customer requests.

4. Communicate the Plan

Effective retail information governance requires a combination of technology and employee awareness. Wherever possible, automate privacy law compliance with filters, retention policies and system alerts. But keep in mind that no automation can fully address the human element.

Make privacy awareness a part of company culture. Communicate the privacy program in multiple ways, from formal training to just-in-time reminders. Ensure that employees at all levels understand the nature of data privacy regulations, as well as the actions they must take to guarantee compliance.

5. Update Documentation

In addition to communicating the privacy program internally, you will need to also update outward-facing documentation. Most privacy law includes requirements for updated privacy policies that are both clear and easily accessible. You will also need to update websites and review vendor contracts.

6. Provide for Ongoing Compliance Monitoring

Compliance and privacy law continues to evolve. Likewise, as retailers incorporate new technologies and expand their business reach, the changes will affect compliance. To prove effective in the long term, privacy programs must provide for ongoing compliance monitoring. With a detailed view into unstructured data, businesses can guard against hefty fines and other complications.

Empower Privacy Law Compliance with Retail Information Governance

For 15 years, Messaging Architects has delivered professional consulting services around data security and information governance. Our compliance experts will clarify emerging privacy regulations. And we will guide you through the process of developing retail information governance strategies to facilitate compliance.

From eDiscovery to comprehensive data security and ongoing compliance monitoring, we offer the tools to help you harness the business benefits of proactive information governance. For more information, stop by the Messaging Architects booth at the National Retail Federation 2020 Vision conference in New York City.