

A red rectangular banner with the text 'Retail Industry Spotlight' in white, sans-serif font. The banner is positioned horizontally across the middle of the image, partially overlapping the hands and the smartphone.The main title of the document is 'Global Privacy, AI, and Data Governance for Resilience and Trust', written in a large, bold, white, sans-serif font. It is positioned in the lower half of the image, overlapping the hands and the laptop keyboard. The background of the entire image is a blurred office scene with a person in a blue shirt holding a smartphone, with various digital icons (shopping cart, coins, bar chart, target, people, gift) floating around the phone, suggesting a focus on retail and digital technology.

Data Governance and Privacy: Key Topics for Retail

In the world of retail, data — especially customer data — is vital. It provides companies with insights into purchasing trends, enables personalized experiences for individuals, and allows retailers to build relationships that deliver value to their customers. But like any valuable asset, customer data is subject to risks and must be protected. From compliance obligations and regulatory penalties to a loss of brand reputation and consumer trust, the numerous risks retailers face continue to evolve.



Key Data and Privacy Considerations for Retail Industry Regulation and Tracking Technology

As more states and international jurisdictions pass new privacy laws and strengthen existing ones, retailers must stay abreast of changes to requirements in tracking technology. That technology includes cookies, banners, tags, pixels, consent management, retargeting, analytics tools, and mobile app tracking. Regulators are looking into whether companies are honoring opt-out choices across retailers' websites, apps, emails, loyalty programs, and paid media.

With at least a dozen states now recognizing the Global Privacy Control browser signal, there has been a notable increase in the scrutiny of retailers' websites. The public-facing nature and accessibility of websites also make them an easily audited area for regulators. Retailers who fail to properly abide by tracking technology requirements — even through unintentional actions such as misconfigurations — can face stiff penalties.

While the U.S. does not have a federal privacy law, individual states continue passing legislation that directly impacts retailers. This results in states such as California and Colorado, which have some of the most robust privacy requirements, creating a de facto baseline for organizations to abide by.

When Does California Require a Cybersecurity Audit?

The California Consumer Privacy Act (CCPA) has brought new cyber audit requirements for businesses that fall into certain criteria:

- ▶ Scope: Annual cybersecurity audits are required for businesses whose data processing activities "present significant risk to consumer privacy or security." Under this categorization, employees are also considered consumers.

Businesses fall within scope when the following apply:

- ▶ 50% or more of annual revenues come from selling or sharing consumers' personal data in the preceding year.
- ▶ As of January 1 of the preceding year, the business has annual revenue of \$26,625,000.
- ▶ Processed the personal information of 250,000 or more California consumers or households in the preceding year.
- ▶ Processed the sensitive personal data of 50,000 or more California consumers in the preceding year.





Automated Decision-Making and AI

Artificial intelligence presents retailers with novel opportunities to engage with their customers and provide enhanced service. From answering product questions online to providing deep personalization to customers, AI can enhance shopping experiences across different platforms and in person. But to function properly, AI needs data, and for retail companies, that data often contains personal information. Retailers must understand what data AI platforms and agents are accessing, how they're using it, and how it's being protected. Additionally, companies need to establish protocols for how they store and govern data, keeping it only as long as they have a business need and is legally required.



Balancing Privacy, Personalization, and Trust

Personalization features aren't just limited to AI-enabled experiences. While AI can enhance those features, customers have been willing to provide retailers with information in exchange for a more customized shopping experience for years.

The willingness of customers to offer personal information comes with an important caveat: When they opt in to sharing their information, customers expect companies to safeguard and handle it responsibly. When retailers apply strong data governance practices, they can effectively use personal data to better understand their customers' preferences and meet demand.



Promoting Data Governance and Privacy

Strong data governance practices can help retailers maintain compliance with expanding privacy laws. There are several steps that retailers can take to help make the compliance process easier, including:

- ▶ Addressing data fragmentation, where data becomes scattered across platforms and systems. Data fragmentation hampers AI use by segmenting data across multiple areas rather than in a single accessible repository. Addressing this allows companies to properly inventory their data, leverage its value, and implement appropriate data protection controls.
- ▶ Building a culture where privacy considerations are part of standard operations. This means creating a culture in which teams understand their responsibilities, note concerns as they arise, and work together to handle privacy-related challenges.
- ▶ Conducting tabletop exercises to prepare teams for real-world situations they may need to respond to in the event of a security incident.



Preparing for the Future

Privacy and trust are inextricably linked. In addition to fulfilling compliance obligations, retailers can demonstrate their commitment to safeguarding customer data by honoring their privacy choices.



Build Trust Through Stronger Privacy, AI, and Data Governance

BDO's [Global Privacy, AI, and Data Governance for Resilience and Trust](#) e-book looks at how leaders can build operational, trackable governance frameworks that support innovation while reducing regulatory, reputational, and business risk.

BDO's [Privacy & Data Protection Services](#) help organizations develop and implement a comprehensive privacy and data protection strategy to maintain global compliance and responsibly handle personal information.

Explore the **Global Privacy, AI, and Data Governance for Resilience and Trust** e-book ►



Have questions or want to learn more? Contact us!

At BDO, our purpose is to be the people you count on to grow with confidence and achieve what matters most. Our professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization. We are proud to be an ESOP company, inspiring an ownership mindset that enables our collective success.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.

© 2026 BDO USA, P.C. All rights reserved.

