

TECH INDUSTRY ALERT

# California Consumer Privacy Act (CCPA): Key 2026 Impacts for Technology Companies

California has finalized significant updates to the California Consumer Privacy Act (CCPA) that took effect January 1, 2026. The new regulations, issued by the California Privacy Protection Agency (CPPA), expand privacy obligations for businesses—particularly technology companies that rely on data, AI, analytics, and automated decision-making. At the same time, the CPPA has signaled a more aggressive enforcement posture, increasing compliance and operational risk for companies that are unprepared.



# Why This Matters for Technology Companies

The updated CCPA framework shifts privacy compliance from a primarily policy-based exercise to an ongoing governance, risk management and operational requirement. Companies should expect regulators to examine not only disclosures, but how data is collected, processed, retained, and used across systems and platforms—especially where automation or AI is involved.

**Key changes include:**

- ▶ Mandatory Cybersecurity Audits (Phased based on revenue, Beginning 2027)
- ▶ Mandatory Privacy Risk Assessments (Effective 2026)
- ▶ New Rules for Automated Decision Making Technology (ADMT) Expanded Consumer Access Rights
- ▶ Heightened Enforcement Environment



## Who Must Comply

The California Consumer Privacy Act (CCPA), as revised effective January 1, 2026, applies to for profit businesses that do business in California and meet any one of the following criteria:

- ▶ Annual global gross revenues exceed \$26.6 million in the prior calendar year
- ▶ Buy, sell, or share the personal information of more than 100,000 California consumers or households, including through digital platforms, websites, applications, or online tracking technologies
- ▶ Derive 50% or more of annual revenue from selling or sharing personal information

A physical presence in California is not required. As a result, many technology companies—including those operating SaaS platforms, data driven services, digital advertising models, AI enabled products, or automated decision making technologies—fall within scope based on their scale, data practices, or interactions with California residents.

## What Technology Companies Should Be Doing Now



Identify high risk data processing and AI/automation use cases



Assess readiness for formal privacy risk assessments



Understand the scope of where California consumer personal information is stored



Review data retention, access, and deletion practices



Align privacy, security, and governance functions

# Bottom Line

The updated CCPA represents a meaningful shift toward operational privacy and cybersecurity governance, particularly for data-driven and AI-enabled technology companies. Early action in 2026 will be critical to managing compliance, risk management, avoiding enforcement exposure, and maintaining customer trust. BDO's Cybersecurity practice can help evaluate the impact of new regulations.

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO 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.

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](http://www.bdo.com).

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

