Lowenstein Sandler

Client Alert

Privacy & Cybersecurity

January 3, 2020

CCPA: What You Need to Know Now

By Mary J. Hildebrand CIPP/US/E

The California Consumer Privacy Act

The California Consumer Privacy Act (CCPA), effective on January 1, is the first comprehensive data protection law in the United States. CCPA protects the "personal information" of California residents, households, and devices (online and offline). If your organization collects or processes this personal information, CCPA may apply whether or not your business has any presence in California. Enforcement actions are handled by the California Attorney General, with the potential for stiff fines. CCPA also allows individuals to pursue private causes of action against a business for a data breach resulting from failure to implement "reasonable security practices," and receive statutory damages without any need to prove actual harm. Our FAQs (below) may be useful as you assess your next steps.

How does CCPA define personal information?

CCPA expands the scope of personal information to include not only the typical categories such as health and financial data, but also business contact data, online identifiers such as IP addresses, device IDs, advertising IDs, tracking data, consumer profiles, commercial information (e.g., purchasing history), internet activity (e.g., search history), geolocation data, biometric data, and other data points. CCPA applies to personal information collected from or about California residents who are clients, customers, suppliers, vendors, employees, and contractors, among others, regardless of the source of such information.

What entities are regulated by the CCPA?

CCPA applies to (1) "businesses" and their affiliates, (2) "service providers," and (3) "third parties" that have relationships with businesses. Compliance obligations are largely driven by the designation of an organization as a business, service provider, and/or third party, as defined in the statute. An organization may have multiple designations depending on the nature of its data processing activities. For example, it could be a business for HR and marketing data, but a service provider for other activities.

Our model is B2B – could CCPA apply to us?

Yes, because CCPA applies to business contact data.

I've heard that some industries, such as health care and financial services, are exempt from CCPA – True?

No *industry* is exempt from CCPA, but *specific categories of data* may be exempted. As one example, data processed by a financial institution under the Gramm-Leach-Bliley Act (GLBA) is not regulated by CCPA; however, all other personal information of California residents processed by the financial institution is covered (e.g., information about employees, business contacts, online activities).

Our organization already complies with GDPR – surely that's enough to cover CCPA?

No. While the General Data Protection Regulation (GDPR) clearly influenced CCPA, there are substantial differences between them. Organizations should be able to leverage some of the work done for GDPR compliance, but compliance with CCPA imposes new and different requirements.

What should we expect in 2020?

The CCPA's effective date is January 1, but there is a 12-month "look-back" for compliance

purposes. Covered organizations are responsible for personal information of California residents collected or received during 2019. Civil actions and enforcement proceedings are likely to focus on that time frame.

During Q4 2019, California passed seven amendments to the CCPA and the Attorney General issued draft regulations. Instead of clarifying the CCPA, these initiatives actually added complexity. California is expected to continue tinkering with CCPA in 2020.

In the absence of any comprehensive federal legislation on data privacy, and the dim prospects for passage of major legislation during this election cycle, 2020 will bring new state laws regulating the privacy and security of personal information. New York state, for example, considered the New York Privacy Act last year, and other states have pending legislation. Unfortunately for U.S. businesses, these state laws are not aligned, raising the prospect of different frameworks across jurisdictions.

About Us

In today's digital world, where data has become a key asset for conducting business, companies continue to face greater privacy and cybersecurity risks. At Lowenstein Sandler, our Privacy & Cybersecurity team helps clients navigate the rapidly evolving, increasingly complex privacy and security law landscape in the United States and the EU, and around the world. Our cross-disciplinary practice draws on the extensive knowledge and experience of lawyers in our Employment, Employee Benefits, Insurance, Bankruptcy, Intellectual Property, and Litigation practices. Our targeted counsel is relevant to companies across diverse industries, such as health care, retail, professional services, communications, financial services, advertising, and entertainment.

Contact

Please contact the listed attorney for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com