A proactive approach

How to prepare for California's sweeping privacy law

INTERVIEWED BY JAYNE GEST

JUSTINE KASZNICA
Shareholder
Babst Calland

(412) 394-6466
jkasznica@babstcalland.com

WEBSITE: To learn more about Babst Calland, visit www.babstcalland.com.

Insights Legal Affairs is brought to you by **Babst Calland**

In 2018, California signed into law the first state-level comprehensive privacy act, the California Consumer Privacy Act of 2018 (CCPA), which goes into effect Jan. 1, 2020. Due to the CCPA's broad scope and reach beyond California, as well as its large fines and penalties for noncompliance, the law is influencing and setting a high bar for data protection practices nationwide. Since the CCPA was signed, several states have proposed or enacted similar legislation, turning privacy and cybersecurity into a patchwork of state-led experimentation.

"More states are developing privacy laws, which will make it difficult for companies to track and comply with every state's privacy act, not to mention the privacy regimes in non-U.S. jurisdictions, such as Europe's General Data Protection Regulation (GDPR)," says Justine Kasznica, shareholder at Babst Calland.

In the absence of a uniform approach to privacy and cybersecurity, businesses need to be aware of the state, federal and foreign laws being introduced and enacted — even if their operations are not yet affected.

Smart Business spoke with Kasznica about how California's privacy law, and others, will impact companies.

How does California's privacy act work?

The CCPA protects consumers who are residents of California, giving them rights to disclosure, access, deletion and control (opt-out and portability rights), as well as imposing a prohibition on antidiscrimination. It also addresses the data privacy rights of children under the ages of 13 and 16.

The CCPA is modeled on the GDPR, articulating similar consumer rights (even if terms differ) and imposing business obligations and enforcement mechanisms. While compliance with GDPR may facilitate CCPA compliance, the two privacy regimes deviate in their definitions of personal information/data, scope of the rights protected, affected organizations, and penalties and enforcement.

The CCPA applies to for-profit entities (and certain nonprofits) that do business in California and collect or direct the collection of personal information of consumers, if such entity:

- Has total annual gross revenue in excess of $25 million a year.
- Receives, sells or shares the personal information of 50,000 or more consumers, households or devices of California residents
- Derives 50 percent or more of its annual revenue from selling personal information of California residents

With the rapidly changing privacy regulatory landscape, how should businesses react?

Companies need to evaluate how they operate and collect, store and process personal information. Many U.S. businesses will need to change their data privacy practices to comply with the CCPA, GDPR and other privacy laws. Even those companies that are not subject to a particular privacy law may be affected if they partner or do business with companies that need to comply with a law, and the obligations pass on by contract.

A pragmatic approach to privacy law compliance would be to:

- Perform a data privacy assessment that captures what kind of personal information an organization collects, for what purpose it is collected and how the information is being used. Achieving consensus on the definition and categories of personal information/data is critical.
- Understand which privacy laws and regulations apply or will apply. If you believe your organization is subject to the CCPA, reach out to experts in legal, risk and IT who can help ensure compliance.
- Work with legal counsel to modernize or update your terms and conditions, privacy policies, cookie and other data collection policies.
- Redesign and deploy new internal and user-facing processes, safeguards and tools to enable individuals to exercise their rights, as required. This may include new communication tools, notices, banners and opt-in or opt-out features, as well as data access, correction and deletion procedures. Be sure to plan ahead; budget time and resources for the changes.

Bottom line: Whether your organization falls within the scope of the CCPA or not, a wait-and-see approach is not a good strategy. Privacy laws are only going to become more important as the landscape evolves, and the GDPR and CCPA are just the beginning. ●