KPMG

Driving change

The time is now to prepare for changes to California's privacy law

California's new, landmark privacy law will mean significant changes for companies dealing in personal data. The law, considered the most stringent in the United States today, is part of a global movement to protect consumers as they share more personal information (PI) as a result of the rapid digitalization of society.

Recent data breaches, and the negative public reaction to them, have underscored the low tolerance consumers have for the perceived misuse of their data, especially as they are constantly being asked to share more and more of it. Governments worldwide are responding to the growing calls for legislation around the protection of personal data. Other jurisdictions are considering similar laws to California's new law and Europe's General Data Protection Regulation (GDPR) to protect consumers.

While many companies must comply with the new legislation, the most successful ones will be the ones that work ahead of the rules—not just to avoid penalties, but also to gain consumer trust and loyalty. The time to start implementing compliance processes and procedures is now.

Background and comparison to GDPR

In June, the California legislature passed AB 375, the California Consumer Privacy Act of 2018 (CCPA or the Act), which will give California residents the right to be informed about what kinds of personal data companies have collected and whether or not it has been shared with third parties.

The CCPA was inspired in part by the European Union's recently implemented GDPR, which took effect in May 2018 and is considered the new global standard for data privacy protection. While similar, there are some distinct differences between the two laws as indicated in the table on page 2.

> "The CCPA represents a sea change for US companies. With California being one of the largest economies in the world, companies will have to better understand their data practices and the impact of the new regulation on their business strategy. Waiting to the last minute is not a viable option."

Doron Rotman
Managing Director, KPMG LLP

CCPA and GDPR - A comparison

Issue	CCPA	GDPR
Covered Entity	Revenues of $25 million; or data on 50k residents/households/devices; or 50% of revenues are from selling PI	Established in the Union; or NOT established in the Union and (offering goods or services to EU residents or monitoring data subject's EU behavior)
General Enforcement Power	California Attorney General	Supervisory authority within each member state
Civil Penalty	A civil penalty of up to $7,500 per violation	Civil penalties as a percentage of gross revenues
Cure Period	Within 30 days of being notified	No cure period provided in the regulation
Breach Notification Timeline	In the most expedient time possible, without unreasonable delay	Controller has 72 hours after becoming aware of the breach
Private Right of Action	A consumer may bring an action to recover damages up to $750 per incident or actual damages, whichever is greater	EU citizen has the right to pursue compensation claims against controllers and processors for damages
Consumer Access Request	Requires two methods for requesting access to information through telephone and website	At least one method to service access request (self service website, email or telephone)
Customer Access Request Timeline	45 days+	30 days+
Do Not Sell My Personal Information - Internet Webpage	Required	Not Required
Offering Incentives in Exchange for Data	Permissible	Permissible - but must be adopted cautiously
Right to Opt Out of Third Party Sales	Yes	Yes
Opt In Consent for Minors	Yes	Yes
Right of Access	Yes	Yes
Right to Delete	Yes	Yes
Right to Data Portability	Yes	Yes
Right of Rectification	No	Yes
Data Minimization	No	Yes
Legal Basis of Processing	No	Yes
Require Data Protection Officer	No	Yes

How (and why) companies should act now

The CCPA only applies to California residents, but the impact is expected to be much broader, including most major companies that deal in consumer data related to California customers as well as organizations that employ California residents, either as full-time employees or independent contractors—a trend becoming more relevant given the growing number of "gig economy" companies operating in California. Organizations may want to consider extending these practices to all U.S. customers instead of trying to segregate and segment California customers, which would add complexity to their IT infrastructure.

We encourage companies to be proactive in responding to changes associated with privacy laws while anticipating what may be ahead as the issue continues to gain traction from various stakeholders, including more conscious consumers and governments. Companies should adopt a principles-based approach that enables them to build privacy strategies and programs that are more resilient to potential changes in laws and regulations.

We recommend companies consider a range of proactive, risk-based measures to detect and address any compliance gaps that CCPA might create, from adopting new policies and procedures around privacy, to hiring more privacy professionals. Organizations should take into account both legal and operational considerations to ensure their data protection and privacy measures are robust, yet have some flexibility to adapt to further changes over time. Based on our experience with similar initiatives (most recently GDPR compliance efforts), organizations should expect significant initial efforts and resource needs, followed by migration to a sustainable operational model, leveraging, as appropriate, automated tools.

With CCPA, the compliance process will become more complex and require companies to invest a significant amount of time and resources to manage compliance. This is just one reason to start taking action immediately.

For example, compliance with the right-to-deletion requirement will require, among other things, assessing whether an exception applies, identifying the various areas (both internally and externally at business partners and service providers) that data is stored, and creating new business processes to honor deletion requests.

Businesses should also review third-party agreements and consider how they might need to be restructured to comply with the CCPA. Internal training will also be required to prepare employees for changes. Businesses will have to adopt consent management systems and be extremely mindful of opt-in, affirmative consent, requirements by minors or their guardians, in order to properly manage data as it flows through the business and third-party computing systems.

The Act might even require some companies to adjust their business models, such as offering consumers incentives in exchange for their data. These changes have substantial financial and operational implications that should not be underestimated and require buy-in and support from the board and executive management.

Key steps to meet compliance

Below is a three-stage process and key foundational activities that organizations can follow, with the help of privacy specialists, to facilitate their organization compliance with the CCPA. Note that the specific activities each organization follows will differ based on their specific starting point, nature of data collection and use, and the organization's risk appetite.

Stage 1: Preparation

- **Perform privacy assessment**
- **Build a privacy governance program**
- **Analyze your business model** as it relates to the use of PI (i.e., offering consumers incentives in exchange for their data)
- **Perform data mapping/data inventory** of all PI collected

Stage 2: Building blocks

- **Build a consumer self-service model** that handles access requests to PI (and portability requirement of this data), opt-out and affirmative consent requests for the sale of PI, and deletion requests in an efficient and automated manner
- **Prepare and update external-facing privacy policy** with required information to satisfy the CCPA
- **Implement privacy-by-design** (and potentially other related risk topics) into formal change initiatives within your organization
- **Review and renegotiate vendor agreements** with third parties that you share or sell PI with
- **Consider the implications** within your organization's IT landscape and security posture

Stage 3: Final measures

- **Finalize self-service, web-based modules** to facilitate consumer self-service requests
- **Finalize incentive plans** for sale of PI (and opt-in consent for minors/parents)
- **Finalize privacy policy** (internal/external)
- **Iterate and improve** privacy-by-design

To be proactive, companies need to embrace data privacy as part of their corporate values

In today's information sharing and information-dependent economy, data is the new currency. Businesses that proactively manage and protect personal data the way users expect will come out ahead of their competition. In the coming years, data protection and privacy will make or break the success of companies.

Getting it right means more than paying lip-service to the new laws. Companies need to embrace data privacy as a corporate value, and embed privacy into the very DNA of the way the company operates. This process takes time, but in the long term will pay dividends as privacy evolves from a differentiator to a base expectation by U.S customers.

> "Privacy done right – putting the customer at the core of your privacy strategy - is a game changer. Regulations like the CCPA, GDPR, and other similar global regulations provide incentive, but compliance should be a by-product, not the end goal, of a well-designed privacy program."

Orson Lucas, Managing Director, Advisory Privacy, Co-Leader KPMG LLP

Contact us

Steve Stein
Principal, Advisory
Privacy, Co-Leader
312-665-3181
ssstein@kpmg.com

Orson Lucas
Managing Director, Advisory
Privacy, Co-Leader
813-301-2025
olucas@kpmg.com

Doron Rotman
Managing Director
408-367-7607
drotman@kpmg.com

kpmg.com/socialmedia