CEP Magazine - June 2020
What legal teams should know about CCPA supplier readiness

By Dov Goldman

Dov Goldman (dov@panorays.com) is the Director of Risk and Compliance at Panorays in Tel Aviv, Israel.

Legal teams are charged with ensuring that third-party business partners, outsourcers, and suppliers comply with regulations. Therefore, it's not surprising that many legal teams are particularly worried about how the newly enforceable California Consumer Privacy Act (CCPA)[1] will shape those relationships.

There's good reason for concern: Businesses that fail to comply could face penalties of up to $2,500 per negligent violation and $7,500 per intentional violation. Individuals can also seek damages of between $100 and $750, and actions can be aggregated into a class action, which may expose a company to enormous financial penalties through its consumers. For these reasons, legal teams must understand the importance of vendor compliance with CCPA and why partners who are noncompliant pose an unacceptable risk.

The regulation

Similar to the way the General Data Protection Regulation defined data privacy in Europe, CCPA is leading the way in US data privacy regulations. Many states have already started to follow California's example by introducing their own, often similar, privacy regulations.

CCPA applies to companies that do business with California residents, whether the organization has a California office or not, and where *at least one* of the following is true:

- Revenue of greater than $25 million;
- Buy, sell, or share the personal information of at least 50,000 consumers, households, or devices, which do not all have to be from California;
- Derive 50% of its annual revenue from selling personal information.

There are numerous exemptions to CCPA; however, it's expected that even those businesses not legally required to comply with CCPA will likely do so anyway. This is because other data privacy laws in the making will mandate similar standards. Moreover, it's best and simplest for businesses to provide the same rights for all their customers, rather than just those who live in California.

CCPA rights

CCPA grants Californians specific privacy rights over their personal data held or processed by businesses and their suppliers. These include the rights to:

1. Know what personal information is being collected about them,
2. Be apprised whether their personal info is sold or disclosed and to whom,
3. Say no to the sale of personal information,

4. Access and delete personal information, and
5. Equal service and price, even if they exercise their privacy rights.

Under CCPA, Californians must provide explicit consent for their data to be used when they are sold from one company to another. People have the right to sue if any of these privacy guidelines are violated, even if there is no breach, and businesses have 30 days to cure alleged violations.

Personal information

CCPA defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

Unlike personally identifiable information, which is a limited set of data types, under CCPA, personal information can include—and is not limited to—names, aliases, postal addresses, online identifiers, IP addresses, email addresses, account names, Social Security numbers, driver's license numbers, passport numbers, biometrics, geolocation data, products or services purchased, browsing history, educational information, and employment information.

Service providers vs. third parties

CCPA makes a distinction between "service providers" and "third parties." *Service providers* receive personal information from a business in order to perform a task with those data, according to the terms of a written contract with a business. A good example would be a mail services company that uses the names and addresses of a company's customers to generate labels.

CCPA requires service providers to be bound by a contract that specifically prohibits using, retaining, or disclosing the personal information for any other purpose beyond the task they were hired to do. A business is not liable for its service provider's conduct if that business has a CCPA-compliant written contract and has no reason to believe that the service provider would violate it.

Third parties receive personal information from a business but are not service providers or part of the business. Such third parties use personal information for their own purposes. Direct marketers are a good example of CCPA third parties. According to CCPA, personal information that has been sold to a third party by a business cannot be resold unless the consumer has received notice and the opportunity to opt out. If consumers demand it, businesses have 30 days to provide a report about what type of information they have.

Best practices for supplier CCPA readiness

Companies that conduct business with suppliers should do the following:

1. Manage data and suppliers

Under CCPA, companies will need to keep better track of their data processing activities. This includes internal business processes and any data shared with suppliers.

Many businesses are often not fully aware of all the assets they own and all the suppliers with which they work. Therefore, it's a good idea to perform a complete audit to map all data and their sources. It is helpful to use a solution that scans information technology systems to discover and map digital assets, as well as uncover subcontractors further down the supply chain. Doing so will help a business develop a clear picture of their

service providers and third parties, as well as these companies' respective digital partners.

2. Check suppliers' compliance

Suppliers will also need to have processes in place to ensure that they can comply with CCPA. A thorough security questionnaire should include questions that specifically address this, including verifying whether suppliers:

- Can quickly access personal data,
- Can correct or erase personal data upon request,
- Maintain up-to-date records of processing activities, and
- Share personal user data with other businesses.

3. Update supplier agreements

Companies will need to have written contracts in place with service providers specifying that customers' personal data may be used for the express purpose of completing a specific task. Such contracts need to stipulate that using, retaining, or disclosing those data for any other purposes is prohibited.

4. Manage cybersecurity

CCPA stipulates that organizations must implement "reasonable" security measures. Therefore, it's important for companies to be able to demonstrate that they have taken steps to reduce the risk of data breaches. It's recommended to use a solution that provides comprehensive automated third-party security management in a manner that allows organizations to:

- Rapidly identify and scan the attack surface of a vendor for potential vulnerabilities,
- Create customized automated security questionnaires and quickly receive responses,
- Detect when vendors don't adhere to the organization's internal security policies,
- Receive actionable insights to mitigate cyber gaps, and
- Receive live alerts about any security changes.

Looking ahead

With many new state and federal data regulations being considered, the United States is clearly moving down a path of greater information security and privacy regulations. For this reason, legal teams should make sure that businesses examine their privacy policies and assess their cybersecurity posture and that of their suppliers. With quality security and privacy controls in place, businesses can rest assured that they will easily align with the security demands of CCPA and other privacy regulations.

About the author

Dov Goldman has years of experience in the third-party risk and compliance field, focusing on the evolving best practices and industry standards in third-party management and regulatory compliance. He has a long history as a serial entrepreneur and software and network engineer. Previously, Dov was vice president of innovation at Opus, director of product marketing at Navigant, and founder and CEO of Cognet Corp and Dynalog Technologies.

Takeaways

- Companies must allow consumers to view, correct, or erase personal information; be informed of whom it was sold or disclosed to; and opt out of its transfer.
- Companies regulated by California Consumer Privacy Act (CCPA) must take responsibility for personal data and their processing, even when third parties are involved.
- CCPA specifies two categories: service providers, who are typically data-processing vendors, and third parties, who aren't vendors but may use personal information for their own purposes.
- Regulated companies must contractually bind service providers to use personal data only for specified purposes and uses deemed in compliance with CCPA.
- Organizations must ensure that third parties they may transfer personal data to are actually compliant with CCPA and may not rely solely on contractual provisions.

1 California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 to 1798.198 (West 2018).