How to Leverage Your Company's GDPR Program to Ensure CCPA Compliance

Compliance and Ethics

The California Consumer Privacy Act (CCPA), one of the most comprehensive US laws to date that is aimed at increasing privacy rights and securing consumer protections, took effect on Jan. 1, 2020. The newly bolstered rights and protections provide a greater sense of “data awareness” among businesses collecting, sharing, or selling a Californian consumer’s personal information. With injunctions, statutory damages, and penalties up to US$2,500 per violation (or up to US$7,500 for each intentional violation) for noncompliance, awareness of this law is critical.

When will enforcement begin?

While the CCPA’s effective date was at the start of the year, the law will be enforced on July 1, 2020. Despite the plea of 60 companies to push the enforcement date back six months in order to alleviate new challenges posed by the COVID-19 pandemic, California Attorney General Xavier Becerra currently has no plans to change the enforcement date.

However, it is important to note that noncompliance with the CCPA, even prior to the enforcement date, may not exempt businesses from penalties. When Becerra was asked about a perceived “safe harbor” for noncompliance that some have interpreted to exist between the CCPA effective and enforcement dates, he stated,

> “If someone is murdered and it takes us six months to arrest whoever did it, does that mean they should go free?... Look, I do not think so. The Law is the law.”

Becerra’s comments are a warning for businesses not to assume there is a “safe harbor” for CCPA noncompliance.

How can your company's legal team expedite CCPA compliance?

In-house counsel should work with business stakeholders to review policies and infrastructure that have previously been implemented as part of its preparation for the EU General Data Protection Regulation (GDPR). The GDPR governs the processing of personal information by EU businesses and businesses processing EU data.

The CCPA emulates several elements of the GDPR, including its security and notice requirements as well as its right to deletion. Given the similarities, certain company GDPR policies and infrastructure may be leveraged to ensure CCPA compliance.

1. Security

Under the CCPA's security requirement,

> "Any consumer whose non encrypted or nonredacted personal information … is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following."

Similarly, the GDPR requires companies to "ensure appropriate security of personal data, including protection of unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."

However, the CCPA, unlike its European counterpart, provides consumers with a limited private right of action for a company's failure to provide reasonable security measures.

The law states, "[a]ny consumer whose nonencrypted and nonredacted personal information … is subject to unauthorized access and exfiltration, theft, or disclosure" due to a business's failure to "implement and maintain reasonable security procedures" may commence a civil action to recover either 1) actual damages; or 2) statutory damages between US$100 and US$750 per consumer per incident (whichever is greater).

The potentially catastrophic financial consequences and civil actions for failing to implement the appropriate data security safeguards should motivate you to act now.

Action items

If your company has implemented or assessed its security measures as part of its GDPR compliance program, it has the foundation to attain compliance with the CCPA's security requirement. Your company should also:

- Collaborate with multiple teams (e.g., security, privacy, IT, and compliance), in order to align best security practices.
- Assess how your company's policies compare to the Center of Internet Security's 20 CIS Controls' proposed security issues (e.g., authentication, data protection policies, and incident response plans).

- Review the security policies of your company's service providers.

2. Deletion

The CCPA provides consumers with a "right to request that a business delete any personal information about the consumer which the business has collected from the consumer." Under the law, after a business receives a "verifiable consumer request from a consumer to delete the consumer's personal information … it must delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

Similar to the CCPA's "right to deletion," the GDPR provides consumers a "right to erasure." Specifically, the GDPR states, "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data…"

Furthermore, the CCPA and the GDPR provide similar exceptions to a consumer's right to deletion, including instances where the information is necessary to:

- Complete the transaction for which it was collected;
- Provide goods or services requested by the consumer;
- Promote free speech; or
- Maintain scientific, historical, or statistical research in the public interest.

Action items

If your business is compliant with the GDPR deletion requirement, it is well positioned to adhere to the CCPA's right to deletion. However, your company should consider the following:

- Ensure the effectiveness of any implemented procedures, IT infrastructure, or technologies that are used to identify and handle deletion requests.
- Review your company's authentication policy to guarantee deletion requests can be properly executed.
- Distribute your company's policy on handling data deletion requests to all employees.
- Implement a self-service tool that allows consumers to make deletion requests.

3. Privacy notices

The CCPA requires businesses to notify consumers of the sources, purposes, and categories of third parties with whom information is shared and the specific pieces of personal information it has collected. Similarly, the GDPR requires businesses to notify consumers of the categories of recipients that receive an individual's data and the purpose for the business to process an individual's personal data.

Action items

If your company's privacy notification is GDPR compliant, it has a solid foundation to achieve compliance with the CCPA's provision on notices. Your business should include the following in its notice:

- The categories of personal information sold or disclosed for a business purpose in the previous 12 months;
- A description of consumers' rights under the CCPA, including access, deletion, and opt-out; and
- A toll-free number for consumers to submit requests for information regarding the collection, selling, or sharing of personal information.

Conclusion

If your business is impacted by the CCPA, your legal team should not wait until the enforcement date to become CCPA compliant, as there is no "safe harbor" between the CCPA effective and enforcement dates. Prioritizing compliance with the CCPA will prevent injunctions and fines that can financially devastate your company.

To expedite compliance, review your company's GDPR compliance program to see if there is any overlap. Finding commonalities between the two laws, combined with additional actions pursuant to the CCPA, will help your company become compliant. The information contained herein does not constitute legal advice, nor does it create an attorney-client relationship.

The information expressed above is an analysis and opinions of certain statutory developments. Such analysis and opinions are mine alone and do not necessarily reflect the opinions held by my employer. If you have concerns regarding such developments, contact a lawyer directly so that your certain circumstances can be evaluated.

Martin Sims

In-House Counsel

NortonLifeLock Inc.

He provides legal support to multiple business units, including: breach response; employer benefits; co-marketing; consumer sales-retail and eCommerce; and global payments. He advises on a wide range of legal topics related to cyber-safety products.