GT GreenbergTraurig

Consumer Privacy Act and Its Implications for Insurers Doing Business in Calif.

Data privacy remains one of the most significant concerns facing the insurance industry. A flurry of new and evolving data security and privacy laws and regulations are re-shaping the regulatory landscape, making it more difficult for companies to avoid exposing themselves to regulatory and other legal risk.

By Francoise Gilbert, Fred E. Karlinsky, and Christian Brito| August 27, 2018 | The Legal Intelligencer

Data privacy remains one of the most significant concerns facing the insurance industry. A flurry of new and evolving data security and privacy laws and regulations are re-shaping the regulatory landscape, making it more difficult for companies to avoid exposing themselves to regulatory and other legal risk. This is especially true for companies that operate on a national level and must comply with the laws of multiple jurisdictions. It is crucial for companies to maintain a culture of compliance by staying abreast of emerging legal and regulatory standards adopted by state legislatures and insurance departments.

Overview

Recently, California enacted the California Consumer Privacy Act of 2018 (CCPA), which becomes effective Jan. 1, 2020. The CCPA was signed into law after being rushed through the California Legislature to block a similar ballot initiative that had garnered sufficient signatures to qualify for the November 2018

election. While both measures contained similar terms, it will be significantly easier for the California Legislature to amend the CCPA than its ballot counterpart.

The CCPA is intended to give consumers more control over their personal information, means to access the records kept by businesses, and to have such information deleted. The CCPA has numerous similarities with the EU General Data Protection Regulation (GDPR). The definition of "personal information" includes a broad list of personal and commercial characteristics and behaviors, as well as inferences drawn from this information.

Like the GDPR, the CCPA provides California consumers with the ability to obtain information about the sharing and disclosure of their personal information and to prohibit such sharing or disclosure. It grants consumers a right of portability and a right of erasure.

The law affects a broad range of entities doing business in California, potentially creating obstacles to their marketing and monetization efforts. Insurers doing business in California (e.g., selling policies to cover insureds or assets located in the California) should become familiar with the CCPA and its requirements and begin preparing to comply with the law.

Scope

The CCPA applies to "businesses." The term is defined as a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that collects consumers' personal information, or on the behalf of which personal information is collected, that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, does business in the state of California, and satisfies one or more of the following thresholds:

- Has annual gross revenues in excess of $25 million;
- Alone or in combination, annually buys, receives, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or
- Derives 50 percent or more of its annual revenues from selling consumers' personal information."

Definition of 'Personal Information'

The definition of what constitutes "personal information" is consistent with the definition of personal data found in the GDPR. Personal information is broadly defined as information that identifies or relates to a consumer or household. The term specifically includes, but is not limited to:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, Social Security number, driver's license number, passport number.
- Commercial information, including records of personal property, purchases, purchasing history.
- Biometric information; geolocation information.
- Internet or network activity information, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.

- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information.
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer.

Obligations for Covered Entities

The CCPA imposes on entities that collect, use, store, share or process personal information of individuals in California significant obligations that go well beyond current common practices. For example, there are significant record keeping requirements as well as limitations to data retention. Businesses will also be required to inform consumers of their rights regarding their personal information and will be required to disclose what personal information is collected and the purposes for which it is used, including whether the information is sold to third parties, the categories of information that is shared with or sold to third parties, and the categories of third parties.

Consumers' Rights

Consumers will have the right to access the information that a business holds about them and the right to request deletion of personal information. A consumer will have the right to request that a business disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of third parties with which the consumer's information is shared or to whom it is disclosed. The consumer must receive a response within 45 days of making a request and providing appropriate identifying information. The provision is similar to GDPR Article 17, which provides for a "right to be forgotten or right of erasure." Businesses will be required to delete the personal information after verifying the identity of the requestor, with exceptions.

Do Not Sell My Information

CCPA grants consumers the right to request that businesses cease sharing or selling their personal information. Websites will have to display a prominent link on their home page, titled "Do Not Sell My Personal Information," which consumers can use to opt-out of the sale of their personal information.

Importantly, consumers will have the right to equal service and price, even if they exercise their privacy rights. Businesses will be prohibited from discriminating against consumers who prohibit companies from sharing their information, such as by charging a fee, except if the difference is reasonably related to value provided by the consumer's personal information. However, businesses may offer financial incentives for collection of personal information.

Enforcement

The law allows for enforcement by the California attorney general, and provides for a private right of action in cases of certain unauthorized access, theft, or unauthorized disclosure of a consumer's personal information that has not been encrypted or redacted. It is widely perceived that the law will increase privacy litigation.

Next Steps

Although future legislative efforts to amend the CCPA are anticipated, a cautious approach is recommended. Companies should educate themselves on the key components of the CCPA and evaluate the extent to which the CCPA might apply to their activities. Once implemented, it will be critical for an organization to demonstrate, through written records and documented technical, physical, and administrative measures, that management and staff understand the CCPA, and that its governance, its lead generation and marketing practices, and its products and services comply with the CCPA when processing personal information of individuals in California.

Businesses are well-advised to audit their processes for the collection and processing of personal information to determine their exposure and compliance needs under the CCPA. To do so, businesses must understand how the entity interacts with personal information of individuals located in California, then identify the changes to be made to comply with the CCPA when collecting and processing such personal information. Some key steps in this process include:

- **Data inventory:** Identify the universe of the personal information at stake.
- **Data mapping:** Identify what happens to each category of personal information, how it is collected, with whom it is shared, how long it is stored.
- **Current internal framework:** Identify the rules that apply to the current uses of the information (e.g., the processes, procedures, contracts that govern these uses).
- **Gap analysis:** Identify discrepancies with the requirements under the CCPA.
- **Risk analysis:** Identify those action items that are the most important/urgent to prioritize the actions needed.
- **Remediation plan:** Identify the steps necessary to remediate the identified gaps.
- **Implementation:** Develop new structures, policies, and documents to address the GDPR requirements.

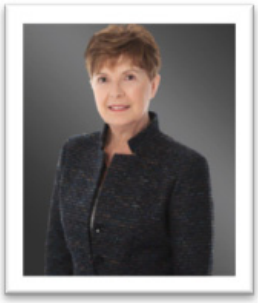
Most companies looking to comply with the CCPA are likely to have to address at least some of the following in connections with their processing of California personal information:

- Understand and address the company's obligations.
- Understand and address the restrictions to marketing, targeting, profiling.
- Update the contracts with data processors, subprocessors.
- Update the privacy notice.
- Develop processes to address obligations regarding individuals' rights.
- Update training for personnel.

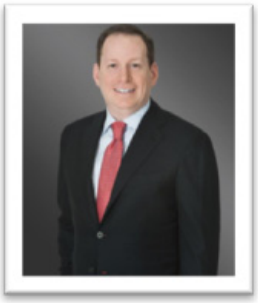
Insurance companies should be prepared to comply with the CCPA if they wish to continue doing business in California. Individuals and businesses located in California may soon inquire whether your company can demonstrate that it meets the CCPA mandates when collecting, using, sharing or processing personal information of individuals located in California. If you are unable to respond adequately to due diligence questions that will be sent to you, potential customers, joint venturers, or investors may take their business to other companies that have made the effort to comply.

About the Authors:

Francoise Gilbert and Fred E. Karlinsky are shareholders at Greenberg Traurig and Christian Brito is a practice attorney with the firm. Gilbert focuses her practice on U.S. and global data privacy and cybersecurity. Karlinsky is co-chair of the firm's insurance regulatory and transactions practice group and Brito focuses his practice on national insurance regulatory and compliance matters.



Francoise Gilbert
gilbertf@gtlaw.com



Fred E. Karlinsky
karlinskyf@gtlaw.com

Christian Brito
britoc@gtlaw.com