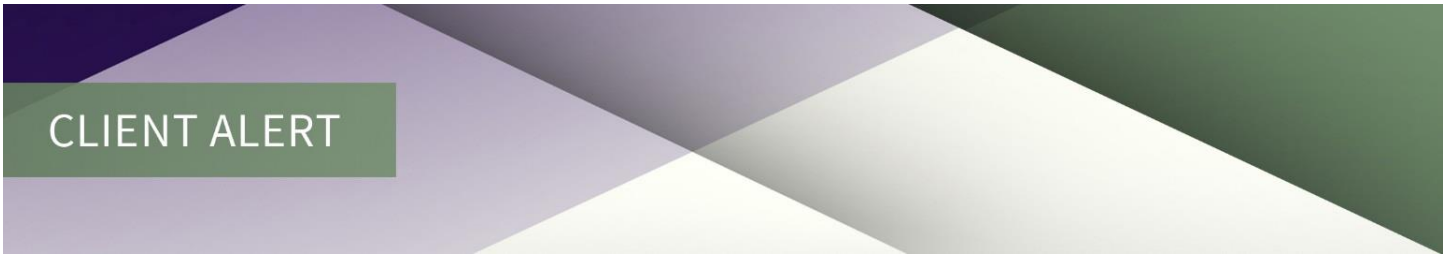

The California Consumer Privacy Act Signed into Law

July 3, 2018

AUTHORS

Daniel K. Alvarez | Alex J. Moyer

After spending two years preparing for the changes wrought by the European Union's General Data Protection Regulation ("GDPR"), many companies must now adjust their sights (and sites) to ensure that their data collection, processing, and disclosure practices also account for the recently enacted California Consumer Privacy Act of 2018 (AB 375) (the "Act"). On June 28, 2018, the California legislature capped off a week of hectic negotiations with stakeholders to enact the Act. The Act contains a number of new privacy requirements that apply broadly to businesses that collect personal information about California consumers and seeks to create new consumer privacy rights.

Companies that already have had to grapple with GDPR will recognize much in the new California law. In particular, the Act is designed to give consumers more transparency and control regarding their data through a series of disclosure requirements for covered businesses and a consent requirement on the "sale" of information. But key distinctions between the Act and GDPR ensure that everybody who collects information from consumers in California will have to pay attention and adjust their practices. While many commentators expect the Act to be revised to some degree in the coming months, the effective date of January 1, 2020, means companies need to start preparing now and make adjustments as warranted.

New Rights for Consumers and New Obligations for Businesses

The Act applies broadly to any for-profit entity that does business in the State of California and collects personal information from consumers in California. There are some exceptions, such as for small businesses (defined as annual gross revenues of less than $25 million), but even a small business may be subject to the Act if it processes the personal

information of 50,000 or more consumers, households, or devices, or derives 50 percent or more of its annual revenue from selling consumers' personal information.

Companies with data collection and processing practices that are subject to the Act need to ensure their practices comport with the new requirements established by the Act. In particular:

- **Privacy Policy Disclosures**: Businesses must post details regarding their collection and use of personal information, including the categories of personal information to be collected, the purposes for which the information will be used, and whether the information will be sold to third parties. This information must be included in a privacy policy that is posted online, and updated annually, along with information about consumers' rights under the Act, the methods to submit requests to exercise those rights, and a list of the categories of personal information that the business has collected, disclosed, or sold in the past 12 months (or the fact that it has not done so). The privacy policy of businesses that sell personal data must also include a section discussing consumers' opt-out rights and a link to the "Do Not Sell My Personal Information" page, discussed further below.

- **Right to Know**: Consumers have a right to request that businesses disclose the following about their personal information, including (a) the categories of personal information it has collected about them; (b) the categories of sources from which the information is collected; (c) the business purpose for collecting or selling the information; (d) the categories of third parties with whom the business shares personal information; and (e) the specific pieces of information it has collected about the consumer. Businesses must provide multiple methods to effectuate these requests (e.g., a toll-free telephone number and a website) and must ensure that individuals responsible for handling these requests are properly trained. Businesses must respond to such requests within 45 days.

- **Right to Delete**: Consumers have a right to request that a business delete any personal information that the business has collected from the consumer. A business's obligation to delete the personal information from its systems (and to direct its service providers to do the same) is limited if keeping the information is necessary for certain purposes, including for internal uses that are reasonably aligned with consumer expectations or compatible with the context in which the information was provided.

- **Right to "Opt-Out"**: The Act requires businesses to provide consumers the right to opt out of the "sale" of personal information. The Act also requires businesses that sell personal information to include a "Do Not Sell My Personal Information" page on their website, with a clear and conspicuous link on the homepage. That page must allow consumers to opt out of having their information sold to third parties. Once a consumer has opted out, businesses are prohibited from requesting authorization to sell that consumer's information for at least 12 months. In addition, the Act prevents businesses from selling personal information of a consumer under the age of 16 without opt-in consent.

Key Differences from GDPR

Although the Act appears to have been inspired in many ways by GDPR, there are a number of differences between the two regimes, both in terms of the rights granted and the procedural aspects.

- Many of the consumer rights granted under the Act, while similar to those under GDPR, are more limited in terms of scope and a business's obligations in responding. For example, the Act limits the deletion right to personal information collected "from" the consumer, as opposed to GDPR's broader right to deletion of personal data "concerning" the data subject.

- The Act also does not adopt many of the procedural requirements imposed by GDPR. For example, the Act does not include detailed requirements dictating the relationship between controllers and processors.

There are, however, three aspects of the Act that are not present in GDPR, and which may have significant impacts on, and create substantial uncertainty for, covered businesses.

- First, the Act specifically prohibits companies from discriminating against consumers who have exercised their consumer rights by denying access to service or charging different prices or rates (including through the use of discounts or other benefits). At the same time, companies are allowed to offer financial incentives that are not unjust, unreasonable, coercive, or usurious. Navigating that line will be a difficult task for many companies.

- Second, the Act provides the Attorney General of California with rulemaking authority to update categories, definitions, exceptions, processes, and more. With input from stakeholders, the Attorney General will thus be able to recalibrate the requirements of the Act to account for changes in environmental and marketplace conditions.

- Finally, the Act establishes a private right of action when a business's failure to maintain reasonable security procedures results in a consumer's personal information being subject to a breach. Under the Act, consumers may recover between $100 and $750 per incident or actual damages, whichever is greater, providing for potentially significant liability for a business suffering a major breach. There are certain procedural steps consumers must follow, including providing businesses a 30-day notice of the violation before filing suit, during which time the business may cure the violation, but it is unclear how useful those provisions will be to companies seeking to avoid potentially costly litigation.

Moving Forward

While many businesses opposed aspects of the Act, they ultimately acquiesced because of the specter of an aggressive privacy ballot initiative (Ballot Initiative No. 17-0039). In particular, the legislative process allows for adjustments to the

Act, while the ballot initiative would not have provided those same opportunities. As a result, business stakeholders are likely to continue to advocate for changes to the Act between now and its January 1, 2020 effective date. In particular, commentators have highlighted several aspects, including the expansive definition of personal information, the private right of action, and some of the specific disclosure requirements, as ripe for changes. Companies, however, should not wait on these efforts to begin the process of coming into compliance with the California law; the lesson of GDPR is that waiting too long to address compliance issues will be more costly than getting ahead of it.

If you have any questions regarding this client alert, please contact the following attorneys or the attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Alex J. Moyer
202 303 1280
amoyer@willkie.com

Copyright © 2018 Willkie Farr & Gallagher LLP.

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.