

California and GDPR “light”: A Match Made in Plaintiffs’ Lawyers Heaven?

Article By:

Blaine C. Kimrey

Bryan Clark

Just when you thought it was safe to open your e-mail again without being inundated with updated privacy policies, here comes the California Consumer Privacy Act of 2018 (“CCPA”). The new law, which goes into effect on January 1, 2020, will expand the privacy rights of California residents and bring some of the EU’s widely discussed General Data Protection Regulation (“GDPR”) to the United States. There will be lots to talk about over the next year and a half as companies gear up for compliance, but here are some key features to be aware of:

- The CCPA does not apply to everyone—it applies only to for-profit entities doing business in California that (a) have annual gross revenues in excess of \$25,000,000; (b) annually process the personal information of 50,000 or more California residents, households or devices; **or** (c) derive at least half of their gross revenue from the sale of personal information.
- The law applies to personal information collected **before** January 1, 2020, as well as information collected after that date. So it’s not enough to make sure your data-handling protocols are sufficient going forward—companies need to make sure they are prepared to apply the new standards to data already in their systems.
- The CCPA includes a much broader definition of “personal information” than is typically seen in the United States, covering “information that identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.” This arguably covers information like IP addresses, e-mail addresses, geolocation data and employment information that typically is not “personal information” under American privacy law.
- The law provides new legal rights to consumers that are usually not seen in the United States, including the right to access personal information, the right to erase personal information, and the right to opt-out of future sale of information.
- The CCPA requires businesses to obtain affirmative opt-ins to sell data of consumers under the age of 16 and businesses are prohibited from discriminating against consumers that

refuse to opt in. Also, under the law, any waiver of the rights provided by the CCPA is unenforceable.

- Importantly, the law provides for a ***private right of action for consumers*** whose personal information was subject to theft or other unauthorized disclosure as a result of a business's failure to reasonably protect the consumers' personal information. Each such incident will allow consumers to recover the greater of actual damages or ***up to \$750 per incident per consumer***. We expect class action plaintiffs' lawyers are already lining up on the courthouse steps in anticipation.

Of course, the CCPA is hardly a full adoption of the GDPR. The CCPA still embraces an opt-out, rather than opt-in, mechanism for most data collection, it does not impose the same requirements on the controller-processor relationship that we have under the GDPR, and thankfully the 72-hour data breach notification requirement is nowhere to be found. But for practitioners wondering how long it will be until the requirements of the GDPR become the global standard, this new law shows it might happen quite soon.

January 1, 2020 will be here before we know it, and any businesses that spent the early part of 2018 scrambling to achieve GDPR compliance know how important it is to be proactive. We will continue to monitor the developments related to the CCPA and stand ready to assist your company in preparing for the implementation of these new requirements.

© 2025 Vedder Price

National Law Review, Volume VIII, Number 194

Source URL: <https://natlawreview.com/article/california-and-gdpr-light-match-made-plaintiffs-lawyers-heaven>