LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

FRIDAY, MARCH 8, 2019

PERSPECTIVE

Consumer privacy across the Atlantic: GDPR vs CCPA

By Mary Race
and Christine Lyon

The California Consumer Privacy Act of 2018 (CCPA) echoes concepts found in the European Union's General Data Protection Regulation (GDPR), but it differs in key respects as well. On one hand, CCPA doesn't cover all of the same concepts as GDPR. On the other hand, CCPA adds new concepts not found in GDPR. All of which raises the question: What do companies need to know about the differences between CCPA and GDPR? If a company has already tackled GDPR, can it feel comfortable that it is reasonably close to complying with CCPA too?

GDPR-style compliance measures can take a company a long way—but not all of the way—toward compliance with CCPA. Below, we describe a half-dozen of the key differences that companies should keep in mind.

First, while CCPA isn't quite as restrictive as GDPR with respect to disclosure of personal information, it does create special new rules for companies that "sell" personal information — i.e., that provide personal information to another business or third party for monetary or other valuable consideration. It is important for all companies — particularly those not familiar with GDPR — to understand the extremely broad meaning of "personal information." CCPA defines "personal information" as any information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This can be as little as a person's name, email address or IP address — even information that is readily available on the internet or from public sources, unless it is lawfully available from certain government records.

If a company sells the personal information of California residents, it must provide an opt-out-of-sale mechanism (or, for minors, an opt-in mechanism) — and, most notably, it must post a "Do Not Sell My Personal Information" link on its website and app. Companies should assess whether they "sell" personal information of California residents and, if so, address the necessary disclosures and opt-out/opt-in rights. Companies should also consider whether they will offer financial incentives to California residents related to use of their personal information and, if so, include the necessary disclosures and opt-in procedure.

Second, many companies updated their privacy notices for GDPR purposes, but CCPA requires different and highly specific types of disclosures in privacy notices and requires updating them every 12 months. Companies should modify privacy notices to address CCPA-specific requirements, such as providing separate lists of personal information categories and new disclosures.

Third, like GDPR, CCPA gives individuals the right to request access to the personal information that a company maintains about them and to receive a portable electronic copy of this information. But, unlike GDPR, CCPA has more detailed content requirements for responding to individual access requests, clear limits on number of times a company needs to respond, and CCPA-specific methods for making and responding to requests.

Similarly, like GDPR, CCPA gives individuals the right to request deletion of personal information that a company maintains about them, subject to certain exceptions. Deletion rights are narrower under CCPA than GDPR, however, as CCPA deletion rights apply only to personal information collected from the individual, as opposed to personal information collected about the individual. Companies should establish access and deletion request procedures to address CCPA-specific requirements regarding response content, timing and delivery. Companies should also provide at least a toll-free number and website address for individuals to submit CCPA access or deletion requests, while ensuring that individuals are not required to create an account to make such requests.

Fourth, CCPA contains an express prohibition on discrimination for the exercise of CCPA rights and new requirements and restrictions around offering financial incentive programs that encourage or discourage how individuals exercise their CCPA rights.

Fifth, CCPA requires that personnel responsible for handling CCPA inquiries be trained on CCPA requirements and how to direct individuals to exercise their CCPA rights. Training key stakeholders on awareness of CCPA rights and requirements is a good first step for any company.

Finally, and importantly, although CCPA contains no new security requirements, it creates new civil penalties and a private right of action related to certain security breaches.

There is still much more to come on the CCPA front, as many CCPA requirements will be clarified or expanded through upcoming rulemaking by the California attorney general. Adding more complexity, there are pending legislative proposals to amend CCPA, including proposals to expand the private right of action. However, the act's effective date of Jan. 1, 2020, is now less than a year away. Companies who have GDPR compliance mechanisms in place can leverage relevant components of their GDPR compliance program as a starting point to address CCPA and then address the incremental additional requirements under CCPA.

For companies that haven't addressed GDPR, the first step may involve figuring out what personal information they maintain and where in order to be able to retrieve or delete personal information quickly in response to a CCPA access or deletion request. This is often no small task, given the plethora of IT systems, databases and vendors that may be used by a single organization. These companies may also need to create new processes for verifying, tracking, and responding to individual requests for access (including portability) and deletion.

With a growing number of states considering similar types of privacy laws, and discussions of a potential federal privacy law gaining momentum, efforts to handle individual requests and track personal information under CCPA should offer benefits that extend beyond CCPA itself. Indeed, such efforts can help lay important compliance groundwork as the world anticipates the next round of headlines announcing the latest data privacy legislation, and companies move toward more global strategies for managing their data.

Mary Race *is an associate and* **Christine Lyon** *is a partner at Morrison & Foerster LLP.*


RACE


LYON