Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

California's Consumer Privacy Act Vs. GDPR

By **Grant Davis-Denny** (August 1, 2018, 1:42 PM EDT)

Grant Davis-Denny

Barely a month after Europe's General Data Protection Regulation went into effect, California lawmakers hastily passed the most aggressive privacy law in the United States, the California Consumer Privacy Act of 2018. (See our previous Law360 article for more information on the CCPA's background and requirements, and key open questions about the law.) Commentators were quick to point out similarities between the CCPA and the GDPR. Meanwhile, business leaders that invested substantial resources in GDPR compliance hoped that their companies would likewise be CCPA-compliant when the California law takes effect on Jan. 1, 2020.

If only life were so simple. While the CCPA's drafters looked to Europe's new law as a model for consumer privacy rights, they did not parrot the GDPR's language, adopt all of its requirements or limit themselves to the GDPR's provisions. Both the CCPA and the GDPR, moreover, contain significant ambiguities that regulators, the business community and consumers will grapple with for years to come. Overlaying the scope of the two laws on one another thus yields a Venn diagram where the common area is significant but ill-defined and where each circle covers distinct areas.

Identified below, are some of the key similarities and differences between the GDPR and the CCPA.

(Somewhat) Common Areas

Although the CCPA generally does not repeat verbatim the terms used in the GDPR, the two laws contain similar concepts.

The Definition of "Personal Information/Data"

Both the CCPA and the GDPR contain incredibly broad definitions of the phrase "personal information" or "personal data," the shorthand phrases the two laws use to describe the type of data to which they apply. Both laws cover nearly all data related to a particular individual, and not just Social Security numbers, health care data or other information that traditionally has been regarded as sensitive. California's law expressly deems such commonly known data as names and physical addresses as "personal information." The CCPA also reaches "consumer's interaction with an Internet Web site," a category of data commonly maintained by companies with an Internet presence. Both laws extend to

data that, directly or indirectly, can be linked to an individual (in the case of the CCPA) or that can be used to identify an individual (in the case of the GDPR).

Although the two laws take a similar approach to defining the scope of data within their reach, there are at least two potentially significant differences. First, California covers information not just about a particular individual, but about a "household" as well. This could have significance, for example, when businesses retain internet protocol address information, which may be difficult to associate with a particular individual but which may be more easily linked to a specific household. Second, California excludes from the definition of "personal information" that data which is "publicly available." (Though California's definition of "publicly available" — information that a government makes lawfully available — is narrow).

Territorial Scope

Both the GDPR and the CCPA purport to regulate businesses located outside the borders of the EU and California. The GDPR attempts to cover businesses that offer goods or services to, or monitor the behavior of, EU residents, regardless of whether the business is located outside the EU. The CCPA's drafters similarly sought to apply that law's requirements to all entities that collect data about California residents and that do business in California (subject to certain thresholds, such as at least $25 million in annual revenue) even if the business does not maintain a physical presence in the state.

Shared Principles

The GDPR and the CCPA grant their respective residents certain rights and impose on businesses certain duties that are, at least at a high level, similar. These shared rights and duties include:

- Right to Notice: Both laws grant residents the right to receive notice of the data that is being collected and how it will be used, and restrict the ability of companies to use data in a way that has not been described in a prior notice. Both laws generally require this notice to be provided at or before the time information is collected from the resident. The GDPR further specifies that if the business is not collecting the information directly from the resident, it must provide the notice within a reasonable period not to exceed one month, the point of the first communication with the resident, or the time of the first disclosure of the data to another party.

- Right of Access: The GDPR and the CCPA also grant residents the right to learn what data companies have about them, the purposes for which the data was collected and the categories of third parties to whom that data has been disclosed. The GDPR adds on that a company must disclose the anticipated period of storage or the criteria that will be used to determine that period, while the CCPA requires disclosure of the specific pieces of data that the company has collected about the collected and the categories of sources from which personal data was collected.

- Right to be Forgotten: Europe and California now allow residents to request that a business delete information about them. Both laws contain exceptions, though their exceptions do not perfectly align. California, for example, allows the company to keep the data if it is being used solely for internal purposes in a manner consistent with the resident's expectations, while the GDPR contains no such exception. The GDPR has a public-health exception, an exception not found in the CCPA.

- Right to Data Portability: Both laws require covered businesses to provide, upon request, a protected resident's data to the resident in a portable format with the goal of allowing him/her to move his/her data to another company. The circumstances in which this right applies and the exceptions vary between the GDPR and the CCPA.

Substantial Potential Liabilities

Both Europe and California's data privacy laws carry high potential liabilities. The type of liability exposure, however, differs between the two laws. In the case of the GDPR, the threat comes from EU member states' enforcement agencies, which can impose fines of up to 4 percent of a company's worldwide annual revenue for numerous types of violations. The CCPA also grants California's regulator — the California attorney general — the ability to impose fines. But at a maximum of $7,500 per violation, those penalties pale in comparison to the GDPR's administrative fines. In the case of the CCPA, the real threat comes from class action plaintiffs and their attorneys, who can recover damages of up to $750 per California resident, per incident for certain types of violations. A data breach involving the data of 1.33 million consumers potentially could generate a demand for $1 billion to resolve a consumer class action brought under the law.

Provisions Unique to the GDPR

GDPR-covered businesses must comply with significant duties that have no analogue in the CCPA. Some of those duties include:

Additional Rights

Under the GDPR, EU residents can force businesses to correct inaccurate data and to supplement incomplete information. Those individuals also can object to having their data used for either direct marketing purposes or altogether when they disagree with the business' claim that its interests outweigh the individuals' interests. The GDPR requires businesses to restrict the processing of data in certain circumstances, such as where a consumer has objected to the accuracy of data or challenged the lawfulness of the processing. The GDPR allows an individual to object to having decisions made that significantly affect him/her based solely on automated processing, such as profiling. The GDPR also generally forbids, subject to certain exceptions, processing of particularly sensitive data, such as race, political opinions and religious beliefs. The CCPA does not address these rights and duties.

Data Protection Officers

A key aspect of the GDPR is its requirement that certain types of businesses, such as those that regularly engage in large-scale monitoring of individuals, appoint data protection officers and notify regulators and data subjects of the DPOs' contact information. DPOs must report to the highest levels of company management, receive from the company resource support and access to information and perform a variety of compliance tasks. The CCPA does not require the appointment of a DPO or any other type of corporate officer or employee, though it does mandate that businesses train employees involved in compliance and responding to customer inquiries about the CCPA.

Assessments and Record-Keeping

The GDPR imposes substantial analysis and record-keeping obligations on covered businesses. For example, businesses using new technologies to process data in a manner that is likely to pose a high risk

to EU residents' rights must perform a data protection impact assessment. And if that data impact assessment shows a high-risk absent mitigation measures, the business must first consult with regulators, who can in turn advise the business on additional mitigation steps or impose remedies, including restricting the proposed processing altogether. Businesses with 250 or more employees are also subject to extensive record-keeping requirements, including documentation of each of processing activity, its purposes, and the persons to whom such information was disclosed. The CCPA does not have these requirements.

72-Hour Data Breach Notification

One area where Europe appears to have modeled California is in imposing breach notification requirements. The GDPR, however, goes further than California's data breach law by requiring companies that have suffered a data breach to notify regulators within 72 hours of learning of the breach (California requires notification to affected individuals in the "most expedient time possible and without unreasonable delay," as well as notification to the attorney general in breaches involving more than 500 California residents. California law does not specify the time period for notifying the attorney general).

Provisions Unique to the CCPA

Although the GDPR extends well beyond the CCPA, the GDPR does not encompass all of the CCPA's requirements. Indeed, the CCPA introduces entirely new concepts to the field of data privacy, including:

Right to Opt Out of Sales

The CCPA creates a new right for California residents to opt out of allowing businesses to sell their data (in the case of minors under 16, businesses will have to obtain affirmative authorization before selling data). The GDPR lacks a provision that specifically addresses a right to opt out of data sales. However, European residents could potentially block sales by exercising their right to be forgotten or withdrawing consent to data processing (where processing was based on consent rather than, for example, a business's claim of legitimate interest).

Nondiscrimination/Nonretaliation

The CCPA generally prohibits businesses from discriminating among California residents based on their exercise of rights set forth in the statute. Thus, businesses cannot deny goods or services, charge higher prices, or provide a different level of goods or services because, for example, a consumer opts out of allowing the business to sell her information. The CCPA, however, contains an exception where the discriminatory treatment is "reasonably related to the value provided to the consumer by the consumer's data," a phrase likely to yield confusion and uncertainty.

Methods of Contact

The CCPA prescribes specific mechanisms that businesses must establish to allow California residents to exercise their new-found data privacy rights. On any webpage that collects personal information, businesses will have to include a "Do Not Sell My Personal Information" link. Businesses also must establish a toll-free number and a website where a California resident can submit data access requests.

Step-Transaction Limitation

California's law requires courts to disregard steps that were component parts of a single transaction designed from the start to circumvent the CCPA's requirements.

Conclusion

Both the GDPR and the CCPA are complex laws that will markedly change the data privacy landscape both within and beyond the borders of their respective jurisdictions. While their expansive scope and areas of overlap invite comparisons, they in fact differ in significant ways that will require businesses operating in both the EU and California to carefully design their data privacy compliance programs to account for the unique requirements of the GDPR and the CCPA.

Grant Davis-Denny is a partner at Munger Tolles & Olson LLP.