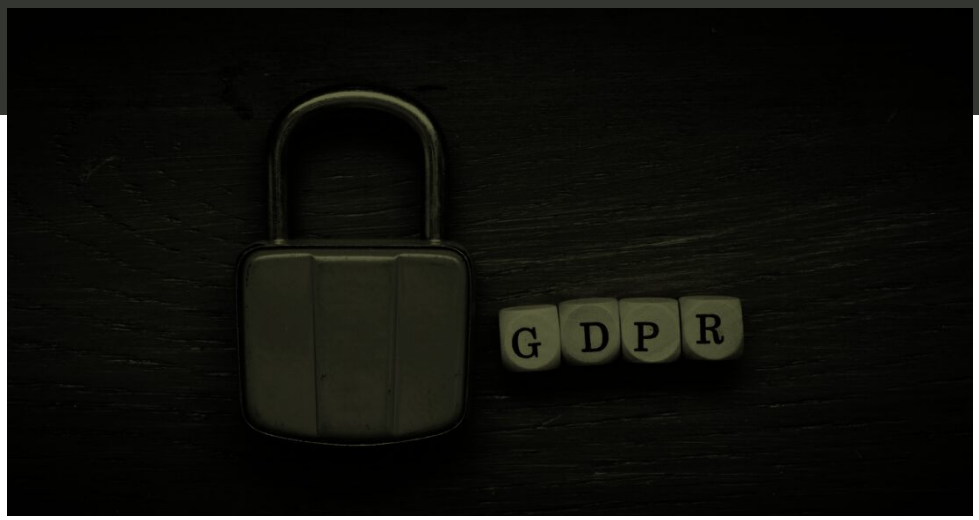
GENERAL

Move Over, GDPR: Here Comes CA's New Data Privacy Law

07.18.19 | Linda J. Rosenthal, JD



Until recently, if you asked random Americans if they recognize the acronym "GDPR," you'd get blank stares and glazed eyes in response.

It's short for "General Data Protection Regulation." Enacted by the European Union in 2016, it went into effect right away, but the drafters included a long transition period: no active enforcement until May 25, 2018.

Beginning in the first half of 2018, people on this side of the Atlantic started hearing chatter – (first, a bit, and then more) – about "GDPR." Then they noticed their email inboxes overrun with messages like: "We've Updated Our Privacy Policy." After that came the annoying pop-ups on websites everywhere demanding consent to said new privacy policies and to "cookies," which most of us now know are not delicious little dessert treats.

So, on March 7, 2018, we posted ***The EU Data-Privacy Law That May Affect U.S. Nonprofits (GDPR)***, giving our readers a heads-up about something important coming down the pike as early as May. We followed up, just after the new year, with ***More About GDPR and Nonprofits*** (January 22, 2019).

GDPR Data Developments

The GDPR had replaced an earlier set of weak security rules and protections for personal data that European Union officials believed were inadequate to meet the burgeoning cybersecurity threats of the internet era.

The General Data Protection Regulation's definition of "**personal data**" is broad, including "anything that can be used to directly or indirectly identify an individual." That can be, for instance: names, photos, email addresses, and social security numbers. It also can refer to "bank details, social media

posts, and medical information."

GDPR regulates the collection, storing, and use of that personal data "**even when it's not being used** for the purpose of rendering goods or services." That's how some charities and nonprofits which collect large amounts of confidential or sensitive private information may be subject to this rule.

A key difference between the GDPR and the earlier law, referred to commonly as the "Directive," is the expansion in certain situations of the territorial reach or jurisdiction beyond the shores of Europe. While the General Data Protection Regulation applies specifically to European Union entities, others based outside of the EU may "**in many cases**" now find themselves subject to its provisions. Specifically, "non-EU-based organizations that **offer goods or services** to individuals in Europe" may find themselves subject to GDPR. This includes certain non-EU nonprofits with donors, grantors, or members in Europe.

American Technology Services, a firm that consults with organizations to help them comply with GDPR, gives **helpful examples** of how or why certain United States nonprofits **may be subject to** this European Union regulatory scheme.

In ***Lands of Confusion? Data Protection Law Changes in the EU and the UK, Part 2*** (May 21, 2019), Greg Duke of Staupell Analytics Group, writes that there is still "a lot of [the] confusion about what GDPR" means for American nonprofits. He had hoped last year that these uncertainties "would be resolved by further instructions from the European Union." That hasn't happened, he laments: "**little has been decided** about the future of [the EU] data protection regulations and what those regulations mean with regards to fundraising institutions in the US."

He cautions, though, that "we should not mistake silence for leniency when it comes to the GDPR. We may not have heard much about data protection with respect to the European Union since last year, but GDPR remains very real and very important for certain U.S. organizations." He adds some good news, though. The specter of potentially "massive fines" may have lessened a bit. In particular, the "EU may have **slightly softened its stance on fines for nonprofits** …. clarifying that fines are the last resort in a 'process' of punishment for data breaches." In the first eight months after the enforcement effective date of May 25, 2018, there were only 91 fines imposed on some 59,000 reported GDPR violations. None of these 91 financial penalties, it appears, were paid by nonprofit organizations.

CA and Other States Take Data Action

Now, on top of what U.S. nonprofits need to know about the European Union's General Data Protection Regulation (GDPR), they should begin paying serious attention to the new data privacy laws in America including – particularly – the **California Consumer Protection Act of 2018**, set to go into effect on January 1, 2020.

While, by its express terms, the CCPA applies to large California corporations that handle huge amounts of private, sensitive data, it will have certain "**cascading effects**." Like the GDPR, it will, in many instances, reach *beyond* the state's borders and *deeper* than the primary, "big business" targets into non-profit-making entities in and outside the Golden State.

In some ways, the CCCA is similar or identical to the EU's General Data Protection Regulation; there are distinctions as well. The California Consumer Protection Act first surfaced as a **proposed ballot initiative** in 2017. As permitted by law, the legislature stepped in the next year to draft and approve its own version that was signed into law by (then) Governor Jerry Brown in late June 2018.

A particularly hhelpful resource for getting acquainted with this new law is the 42-page *California Consumer Protection Act (CCPA) Practice Guide*. There are useful tables and charts that compare and contrast the proposed ballot initiative as first drafted with the final legislative language; "there are significant differences …." Generally, "the version passed by the legislature conferred greater data privacy protections, but imposed weaker penalties for non-compliance." And the CCPA *doesn't* include a data-breach-notification requirement because California already has a separate law on that topic.

Also in the Practical Guide are explanations of the similarities with and differences from the European Union's General Data Protection Regulation.

Not only are several additional states poised to adopt (or have already adopted) legislation modeled after the California law, but the CCPA "will **significantly alter the data privacy landscape in America**." Along with the GDPR, it sets an emerging "best practices" standard for all entities. Although the CCPA is **not directly aimed at nonprofit entities**, the law "… impacts most nonprofits' handling of consumer data, donor information, website user identifiers, and other types of personal information."

> *"Accordingly, **nonprofits all over the United States**, as well as international nonprofits who partner with California entities, should proactively implement key components of data privacy compliance, such as through accurate online disclosures, appropriate user opt-out options, and special care in handling the information of minors."*

Taking these steps should help position nonprofits around the nation to meet the **growing consensus** that is or will be reflected in legislation in the various states and at the federal level and to identify when certain of their operations or structures may "trigger requirements for … compliance with CCPA" and other statutes.

Conclusion

While "**at first blush,** it would appear that CCPA is not relevant to nonprofit organizations" nor does it "expressly require nonprofits to comply with" it – (and it's directed primarily to entities in *California*) – "prudent nonprofits" around the nation should understand its importance, relevance, and their possible liability in connection with it.

In later posts, we'll explore this topic more thoroughly and keep you updated on developments.