Businesses not grasping details of ‘one of the strictest privacy laws in the country’

by Alicja Grzadkowska 18 Nov 2019

SHARE

As the year draws to a close, many businesses and cyber insurers are preparing for the California Consumer Privacy Act (CCPA), whose compliance deadline is set for January 01, 2020 with a six-month grace period before enforcement of the law officially starts.

According to PwC, the top five CCPA requirements that will likely have the most significant impact on companies serving or employing California’s residents include data inventory and mapping of in-scope personal data and instances of selling data, newly introduced individual rights to data access and erasure as well as to opt-out of data selling, the updating of service-level

agreements with third-party data processors, and remediation of information security gaps and system vulnerabilities.

Read more: Many organizations still unprepared for the California Consumer Privacy Act

In essence, the law allows any California consumer to see all of the information a company has collected on them, as well as a comprehensive list of all the third parties with whom that data has been shared. Understandably, this incoming law is a game-changer for the privacy landscape in the United States, so if they haven't already, businesses should take note.

"It is one of the strictest privacy laws in the country and I would suspect that many US businesses do not fully grasp all the core requirements with it so far. I think the key things that they should be paying attention to would be, first of all, whether the law applies to the company. The Act requires businesses to be a certain size – [with] annual gross revenues of over $25 million – or they have to have a bunch of California consumer information for the law to apply," said Michael Palotay, chief underwriting officer for Tokio Marine HCC's cyber and professional lines group, adding that the CCPA likely won't be the last privacy law to come into effect. "With that being said, we're expecting other states to release copycat laws over the next few years, so if you don't have any California information, you still might have to worry about these new restrictions. It's definitely something that people need to be taking seriously."

The implementation of data tracking systems is one of the labor-intensive processes associated with compliance, which can put an additional burden on companies.

"They have to create processes that really can inventory data because the Act allows for a consumer to request to have their information basically deleted from a company's servers and databases," said Palotay. "Especially when a lot of internet-based companies have designed their entire business model on trying to collect as much data as possible, it can be challenging to figure out where all of that is."

While the CCPA's broad privacy requirements are completely new to the US, it's not the first law to set out privacy provisions. The General Data Protection Regulation (GDPR) in the European Union, which came into effect in May 2018, made many businesses perk up their ears since it was the strongest data protection regime in the world, with extra-territorial reach that applied strict regulations on any company offering goods or services to EU residents or monitoring the behavior of EU residents.

However, Palotay has yet to see a wave of regulatory issues or claims stemming from GDPR non-compliance, which might foreshadow what we'll see following January 2020.

"That is a function of a lack of, or limited resources for enforcement and the fact that a lot of companies took it seriously and really incorporated the necessary policies within their business," he told *Insurance Business*. "A lot of these laws are really all about enforcement and the government has limited resources, so that's always something we're watching closely."