Articles
March 23, 2020
CCPA & COVID-19: A Practical Guide to Addressing Privacy and Data Security Implications of the Coronavirus

COVID-19 arrives just as the first omnibus privacy statute in the United States, the CCPA became effective. Since its January 1 effective date, we continue to wait for finalization of the CCPA regulations and enforcement that was slated for July 1. In a pandemic environment, companies, employers, and public institutions are grappling, outside the HIPAA context, with unique privacy, data security, and cybersecurity implications of their responses to the coronavirus. From a compliance perspective, businesses are considering under what circumstances they can disclose consumer or employee health conditions or geolocation information in the service of greater public health. Other companies—and governmental institutions at every level—are confronting the very real, and often opportunistic threats to data security posed by aggressive thieves who use crises as cover to commit an assortment of cybercrimes. Privacy and security requirements vary by jurisdiction, so businesses should be mindful of potentially divergent and overlapping approaches and responsibilities as the situation continues to evolve.

We offer a few updates and practical tips for best practices to promote compliance with privacy and data security requirements.

To read the full article on *PrivSec Report*, click here.

This article was originally posted on *Privacy Quick Tips* on March 19, 2020.

Authors

Explore more in

Privacy & Security