Blogs
March 19, 2019
Perkins on Privacy

Cybersecurity, GDPR, and CCPA

The GDPR and the CCPA have made headlines for their wide scope and impact on privacy practices. On the issue of data security, they take somewhat different approaches, but the bottom line for companies is quite similar: data security measures tailored to the company's risk profile and actual practices are essential for both legal compliance and the protection of the company and its customers. The GDPR makes data security a general obligation for all companies processing personal data from the European Union (EU) by requiring controllers and processors to implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk" (Article 32). As stated in the GDPR, such measures include: pseudonymization and encryption; ability to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services; ability to timely restore availability and access to personal data in the event of a physical or technical incident; and processes for regularly testing, assessing, and evaluating the technical and organizational measures to ensure the security of processing. Comprehensive internal policies and procedures are thus crucial for all companies controlling or processing EU personal data. Recent enforcement brings home this point, as the Portuguese supervisory authority (CNPD) fined a hospital for using software that provided inadequate patient protections, even though the hospital asserted that it used the software provided by the Portuguese Health Ministry. The CCPA, in its current form, makes little mention of data security and contains no specific requirements to secure personal data. Rather, the obligation to "implement and maintain reasonable security procedures and practices" arises in the context of the limited private right of action available when a subset of personal information is breached as a result of a failure to implement such procedures and practices. (Cal. Civ. Code § 1798.150, Cal. Civ. Code § 1798.81.5). This obligation exists in concert with the Federal Trade Commission's (FTC) general authority under Section 5 of the FTC Act to protect consumers from "unfair" practices, including unreasonable data security. Under either regime, what constitutes "reasonable" or "appropriate" data security depends on the organization and the types of data it handles, and there is no one-size-fits-all approach. However, there is a considerable amount of guidance available, particularly with regard to basic precautions expected to be implemented in most circumstances. For example, in the February 2016 " California Data Breach Report," the California attorney general recommended that organizations implement the 20 controls in the Center for Internet Security's Critical Security Controls, affirmatively stating that the failure to implement such controls would constitute a lack of reasonable security. The FTC's "Start with Security" is also a great resource and shares important themes from previous FTC cases involving unreasonable security. European data protection authorities have also issued guidance regarding appropriate security measures, such as the Cyber Essentials guidance document promulgated by the UK's data protection authority. Each of these resources covers similar measures that protect against a wide swath of frequently encountered data-related incidents. Cybersecurity risk management and compliance are moving targets as technological advances will require organizations to periodically revisit their cybersecurity strategies; however, these resources provide organizations a starting point to protect themselves and their customers in addition to enhancing their legal compliance.

Explore more in

Privacy & Security
Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's Privacy & Security practice, recognized by Chambers as a leading firm in the field.

View the blog