GDPR-like Privacy Protection Is Coming to U.S.

07.05.2018

The state of California recently passed privacy legislation that imposes stringent requirements on organizations that collect personal information from California residents. The California Consumer Privacy Act of 2018 (CCPA) imposes protections that are similar to the General Data Protection Regulation (GDPR) that went into effect in Europe in May. For example, under the CCPA, businesses must:

- inform consumers of the categories of personal information that they are collecting and the purposes for which the personal information shall be used;
- upon a consumer?s request, promptly take steps to disclose and deliver, free of charge to the consumer, the personal information and delete any personal information the business has collected from the consumer;
- not sell a consumer?s personal information to third parties upon request, and if a business does sell personal information, provide a clear and conspicuous link on the business homepage, titled ?Do Not Sell My Personal Information?; and
- make available to consumers two or more designated methods for submitting requests for information including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.

The CPSA provides several exceptions to these requirements. For example, a business shall not be required to comply with a request to delete personal information if it is necessary to:

- complete the transaction for which the personal information was collected;
- detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity;
- comply with a legal obligation, such as the California Electronic Communications Privacy Act; or
- otherwise use the consumer?s personal information internally in a lawful manner that is compatible with the context in which the consumer provided the information.

Personal information is defined as ?information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household? and includes several examples. The CCPA applies to businesses that (i) have more than twenty-five million dollars ($25,000,000) in gross revenues, (ii) alone or in combination, annually buy, receive or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices, or (iii) derive 50 percent or more of their annual revenues from selling consumers? personal information.

The CCPA also imposes on businesses an obligation to implement ?reasonable security procedures and practices.? In the event of ?an unauthorized access and exfiltration, theft, or disclosure? of personal information, individuals can recover damages ?in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty dollars ($750) per consumer per incident or actual damages, whichever is greater.?

Although the CCPA is similar to the GDPR, it differs in several important respects. For example,

- the term personal information does not apply to ?information that is lawfully made available from federal, state, or local government records.?;
- it allows businesses in some instances to charge different prices by discounting for those who do not opt out;
- there is no right to a private cause of action, other than for data breaches; and,
- businesses in some cases can ?offer financial incentives, including payments to consumers as compensation,? for collecting and selling their personal information.

While the law does not go into effect until January 1, 2020, companies that collect personal information on residents of California should not wait too long to determine what steps they must take to become compliant. As the GDPR process has shown, it can take a while for businesses to determine what data assets they have and how to address the requirements from both a technical and operational standpoint. In addition, the Federal Trade Commission (FTC) has announced that it will hold aseries of hearings on consumer privacy. The purpose for the hearings is to determine ?whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy.?

Related People

- Kevin D. Pomfret ? 703.760.5204 ? kpomfret@williamsmullen.com

Related Services

- Data Protection & Cybersecurity
- Intellectual Property