Cannabis, Privacy, and Data Security

Overview

Companies that serve consumers in the medical and adult use cannabis industries collect and handle personal information from thousands of individuals. Many cannabis companies – especially multi-state operators and companies that sell CBD online – collect personal information from residents of several different states. If your cannabis company does not maintain adequate data privacy and security practices, you risk enforcement actions from federal and state regulators and reputational harms that could result in lost business and class action litigation. These risks are not hypothetical: information security breaches have caused dispensaries to expose the personal information of tens of thousands of individuals.

Laws & Regulations

- State cannabis laws and regulators are increasingly focused on privacy and data security issues. License applications often require companies to describe their data security practices and abide by representations they make in seeking licensure. And some states, including Illinois, prevent dispensaries from collecting or sharing customers' personal information without consent.
- Every state has laws that govern how companies must prepare for and/or respond to information security incidents. For example, Massachusetts requires companies to maintain a Written Information Security Program detailing their plans for responding to cybersecurity incidents. New York maintains similar requirements alongside a broad definition of wat constitutes a breach of security
- States are beginning to enact comprehensive data privacy laws that govern how businesses collect, use, and share personal information. The California Consumer Privacy Act ("CCPA") creates consumer rights to access, delete, and prevent sales of personal information. Cannabis companies looking to operate in Europe must comply with the EU's General Data Protection Regulation ("GDPR").
- Marketing activities, such as through text messages to consumers, can create significant liability under the Telephone Consumer Protection Act ("TCPA"), leading to significant litigation and nuisance claims.
- The Federal Trade Commission ("FTC") and states Attorneys General have authority to police companies that maintain inadequate data-security or data-privacy practices

How Foley Hoag Can Help

Foley Hoag has a dedicated and experienced Privacy and Data Security team, including attorneys who are Certified Information Privacy Professionals and who have experience in advising cannabis companies on other regulatory and compliance Our team can help cannabis companies with:

- Development and review of privacy and security policies and practices.
- Permissible uses of personal information in marketing, including TCPA compliance.
- Compliance and training for jurisdiction-specific privacy and security laws, such as the CCPA, the GDPR, and various states' breach notification laws.
- Data security breach preparedness and response.
- Diligence reviews of data and security practices in mergers and acquisitions.

Christopher Hart
Partner | Co-Chair, Privacy & Data Security Practice Group | Certified Information Privacy Professional
617.832.1232
chart@foleyhoag.com

Colin Zick
Partner | Co-Chair, Privacy & Data Security and Health Care Practice Groups
617.832.1275
czick@foleyhoag.com

Jeremy Meisinger
Associate | Privacy & Data Security Practice Group | Cannabis Practice Group
617.832.3029
jmeisinger@foleyhoag.com

Jennifer Yoo
Associate | Privacy & Data Security Practice Group
617.832.1709
jyoo@foleyhoag.com