COLORADO

Lance G. Eberhart
HALL & EVANS, LLC
1001 Seventeenth Street, Suite 300
Denver, CO 80202
Phone: (303) 628-3470
Cell: (XXX) XXX-XXXX
Fax: (303) 628-3368
Email: eberhartl@hallevans.com
www.hallevans.com

1. What is your state’s law on the use of CBD oil in products to be sold to the public, i.e. cosmetics, etc.?

I. CBD, or Cannabidiol, is one of more than 100 compounds found in cannabis. THC or tetrahydrocannabinol is the main psychoactive component of the cannabis plant. CBD is a non-psychoactive compound which can be derived from either the marijuana plant or from the hemp plant, and depending on how the CBD products are manufactured, will determine whether it is governed by Colorado’s Industrial Hemp Regulatory Program, or Colorado’s Retail Marijuana Code.

II. Colorado’s Industrial Hemp Regulatory Program is codified beginning at C.R.S. § 35-61-101. Industrial hemp is defined as “a plant of the genus cannabis and any part of the plant, whether growing or not, containing a delta-9 tetrahydrocannabinol concentration of no more than three-tenths of one percent on a dry weight basis.” C.R.S. 35-61-101(7) (2018). Under Colorado’s Industrial Hemp Regulatory Program, a registrant can engage in industrial hemp cultivation for commercial purposes or grow industrial hemp for research and development purposes. C.R.S. § 35-61-102 (2018). By the plain language found in the Industrial Hemp Regulatory Program, “a person engaged in processing, manufacturing, selling, transporting, possessing, or otherwise distributing industrial hemp… or selling industrial hemp products produced from it, is not subject to any civil or criminal actions under Colorado law for engaging in such activities.” C.R.S. § 35-61-108(3) (2018).

III. The Constitution of the State of Colorado provides for the legalization of marijuana and its regulation. See Colo. Const. Art. XVIII, Section 16. At the outset it is stated that in “the interest of enacting rational policies for the treatment of all variations of the cannabis plant, the people of Colorado further find and declare that industrial hemp should be regulated separately from strains of cannabis with higher delta-9 tetrahydrocannabinol (THC) concentrations.” Id. The clear intent that industrial hemp should be regulated separately is repeated when hemp is excluded from the definition of marijuana, as “marijuana does not include industrial hemp, nor does it include fiber produced from the stalks, oil, or cake made from the seeds of the plant, sterilized seed of the plant which is incapable of germination, or the weight of any other ingredient combined with marijuana to prepare topical or oral administrations, food, drink, or other product.” Id.
IV. CBD products which are derived from the marijuana plant, rather than the hemp plant, are subject to the additional testing, labeling, and preparation requirements governing all marijuana products. See C.R.S. § 44-12-202. Part of the Retail Marijuana Code includes a “marijuana products independent testing and certification program… requiring licensees to test marijuana to ensure a minimum that products sold for human consumption do not contain contaminants that are injurious to health and to ensure correct labeling.” C.R.S. § 44-12-202(3)(IV).

V. CBD products are legal in Colorado. However, how such CBD products were manufactured will dictate whether the product is considered a marijuana product or a hemp product.

2. Regarding privacy issues, has your state adopted its own version of GDPR or how is your state dealing with GDPR requirements? What other privacy laws has your state adopted recently in response to concerns about the lack of protections for consumers?

I. Colorado has enacted a strict data-privacy law that went into effect on September 1, 2018. The law requires businesses to develop a written policy governing the disposal of personal identifying information, to investigate possible security breaches, and to notify any person impacted by a security breach, as well as notifying the Colorado attorney general’s office. The bill—H.B. 18-1128, titled An Act Concerning Protections for Consumer Data Privacy—was enacted on May 29, 2018. It amends several existing Colorado statutory sections as well as creating new ones.

II. The first requirement of the bill is that all “covered entities” “develop a written policy for the destruction or proper disposal” of electronic or paper records containing “personal identifying information.” Colo. Rev. Stat. §§ 6-1-713(1). A business need not develop a new policy if the business is regulated by a state or federal law and has already developed a policy to dispose of personal identifying information that conforms with that regulation. Id. § 713(3).

III. The law’s second requirement is that covered entities “maintain reasonable security procedures and practices,” appropriate for the nature of the information and the nature and size of the business, to protect personal identifying information. Colo. Rev. Stat. § 6-1-713.5(1). The business must also require that any third-party provider that handles the business’s data implements and maintains security procedures and practices. Id. § 713.5(2). And as above, a business that is regulated by a state or federal law and already maintains security procedures and practices that conforms with that regulation need not develop new procedures and practices.

A. “Personal identifying information” is defined broadly, to include: a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver’s license or identification card number; a government passport number; biometric data; an employer, student, or military identification number; or a financial transaction device. Id. § 713(2)(b).

B. For the purpose of developing the destruction policy and maintaining security procedures, “covered entity” includes any business that maintains, owns, or licenses
personal identifying information in the course of the entity’s business, except third-party businesses that provide these services. *Id.* § 713(2)(a).

III. The law also implements stringent notice and reporting requirements for data breaches as its third requirement. Colo. Rev. Stat. § 6-1-716. These requirements are expansive. The statute applies to any entity that “maintains, owns or licenses” personal information during its business. *Id.* § 716(1)(b). “Personal information,” in turn, includes a large amount of data: a Colorado resident’s first name or initial and last name in combination with various forms of identification; information that would allow access to an online account; or information that would allow access to a financial account or the use of a credit card. *Id.* § 716(1)(g).

A. Any business that discovers a data breach involving personal information of a Colorado resident must conduct an investigation to determine whether any of the personal information “has been or will be misused.” *Id.* § 716(2)(a). The entity must also give notice of the breach to the Colorado resident unless the investigation determines that no information has been misused and it is not reasonably likely to be misused. *Id.*

B. This notice must be sent to the Colorado resident within thirty days of determining that a security breach occurred, with limited exceptions for delays requested by law enforcement due to a criminal investigation. *Id.* § 716(2)(a), (2)(c). There are also specific requirements for what the notice to Colorado residents must include. See *Id.* § 716(2)(a.2)–(a.4). The notice requirement also applies if the breach exposed “secured personal information” and also exposed the means to decipher that information. *Id.* § 716(2)(g).

C. In addition to notice to the Colorado resident, the business must also give notice to the Colorado attorney general within thirty days of determining that breach occurred if the business believes the breach affected five-hundred or more Colorado residents, unless the investigation determines that no information about a Colorado resident has been misused and likely will not be misused. *Id.* § 716(f).

D. And if the business would be required to notify more than one-thousand Colorado residents of the breach under this law, the business must notify “all consumer credit reporting agencies” that compile data on a nationwide basis of the “anticipated date of the notification to” Colorado residents and the approximate number of residents that will be notified.

E. The law also bars any waiver of the notification rights or responsibilities as void as against public policy. *Id.* § 716(2)(e).

F. A business that already has notification procedures in place may continue to use them if the procedures comply with the timing and notice requirements of the law, but the business must still notify the Colorado attorney general, if applicable. *Id.* § 716(3)(a). Businesses that are regulated by state or federal laws or regulations and that maintain procedures for a security breach in accordance with those laws or regulations are compliant but must still notify the Attorney General, if applicable. *Id.* § 716(3)(b).
IV. The Colorado attorney general is empowered to bring civil actions or to seek economic damages to enforce this law. *Id.* § 716(4). Further, after the attorney general’s office receives the notice required by this law, the office may prosecute violations of state criminal law, if factually appropriate. *Id.* § 716(5).

V. At this point, there is no published case law interpreting or limiting these provisions.

VI. Any business that has clients who are Colorado residents should consider whether the business’s existing policies and procedures conform with this law and should update its policies and procedures accordingly.