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.?**


There are restrictions on the sale of CBD oil derived from marijuana: (1) age restrictions on buyers; (2) tetrahydrocannabinol (THC) content limits; and (3) where CBD can be purchased. First, marijuana-derived CBD oil may not be sold to minors under 21. Or. Rev. Stat. § 475B.005(c). Exceptions to the age requirement apply if the minor holds a valid medical marijuana or designated primary caregiver card. Or. Admin. R. 845-025-8520 (2017). Second, the Oregon Health Authority has the power to set guidelines for the maximum THC content that can exist in CBD oil. Or. Rev. Stat. § 475B.625. For example, cannabinoid edibles can contain up to 100 mg of THC per container; topicals can contain up to 6% of THC per container; and tinctures, capsules, and all other cannabinoid products can only contain up to 4,000 mg of THC per container. OAR 333-007-0220, Table 2 (2017). Third, CBD oil derived from marijuana is sold only at state-licensed dispensaries. Or. Rev. Stat. § 475B.005(1)(c).

The sale of CBD oil derived from hemp, however, does not have as many restrictions. Hemp-derived CBD contains 0.3% or less of THC. H.B. 4089, ch. 116, § 27(5)(a), 2018 Or. Laws. Hemp-derived CBD oil is also more widely accessible: it can be sold in vape stores, food stores, and even through online retailers. *Id.*
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?


A breach of security is “an unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information.” Or. Rev. Stat. § 646A.602(1)(a) (2018). Personal information includes a person’s first name or first initial and last name, combined with at least one or more listed items. Or. S.B. 684 § 2(12)(A). The listed items include a social security number, a driver’s license or state identification number, a passport number, or financial account information. Id. at § 2(12)(A)(i)-(iv). Financial account information includes “any other information or combination of information that a person reasonably knows or should know would permit access to a consumer’s financial account.” Id. at § 2(12)(a)(iv). The 2019 amendment added a username and the means to authenticate a username as personal information. Or. S.B. 684 § 2(12)(a)(B).

If there is a breach of security, someone who owns, licenses, and now “otherwise possesses” someone’s personal information in the course of business must provide notice of the breach. Or. Rev. Stat. § 646A.604(1). The 2019 amendment defines the person who “owns, licenses, maintains, stores, manages, collects, processes, acquires, or otherwise possesses” personal information in the course of business as a “covered entity.” Or. S.B. 684 § 2(5)(a).

Also, notice must be provided if the covered entity received a notice of a security breach from a secondary company. The secondary company is defined in the 2019 amendment as a “vendor.” Id. at § 2(19). A vendor uses a customer’s information “for the purpose of, or in connection with, providing services to or on behalf of the covered entity.” Id. A vendor who holds information on behalf of the covered entity must notify the covered entity of the breach no later than 10
days after discovering a breach or after having reason to believe a breach might have occurred. Or. S.B. 684, § 3(2)(a). A covered entity usually has to provide notice of a breach only to the “consumer to whom the personal information pertains.” Or. Rev. Stat. § 646A.604(1)(a). However, if more than 250 Oregonians’ information has been breached, the covered entity must also notify the Oregon Attorney General. Or. Rev. Stat. § 646A.604(1)(b).

Notice of a breach must be provided to an affected consumer no later than 45 days after a covered entity discovers or is notified of a breach. Or. Rev. Stat. § 646A.604(3)(a). Along with the notice, the company must take “reasonable measures that are necessary” to (a) discover the contact information of the person receiving the notice; (b) explore the scope of the breach; and (c) restore the “reasonable integrity, security, and confidentiality” of the person affected by the breach. Or. Rev. Stat. § 646A.604(3)(a)(A)-(C). Delay of notice is permitted only if law enforcement finds that notification may impede a criminal investigation. Or. Rev. Stat. § 646A.604(3)(b). Notice must be given either in writing, electronically (if that is the customary means of communication), or by telephone (so long as there is direct contact). Or. Rev. Stat. § 646A.604(4)(a)-(c).