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.?**

Effective March 20, 2017, industrial hemp is a legal and viable agricultural crop in Kentucky. KRS § 260.852. Pursuant to House Bill 197 which was enacted on March 21, 2019, industrial hemp “means the plant Cannabis sativa L. and any part of that plant, including the seeds thereof and all derivatives, extracts, cannabinoids, isomers, acids, salts, and salts of isomers, whether growing or not, with a delta-9 tetrahydrocannabinol concentration of not more than three-tenths of one percent (0.3%) on a dry weight basis.”

In order to cultivate, handle, process, or market industrial hemp, a person must first obtain a license issued by the Department of Agriculture. KRS § 260.858(3). In the event that a person engages in these activities without a license, they will be prosecuted and face the same penalties as a person who engages in cultivating, handling, processing, or marketing marijuana. *Id.*

CBD oil is legal in Kentucky and is not included under the definition of “marijuana.” 40 KRS 218A.010(27). Pursuant to Kentucky hemp regulations, CBD oil may be used in a product derived from industrial hemp as described in the above definition. *Id.* at 27(e). Therefore, products are permitted to be sold to
the public if the person or business that is selling and marketing the product has a license from the Department of Agriculture and if the product has a THC content of no more than 0.3 percent.

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?

The General Data Protection Regulation (GDPR) is a European Union initiative to provide EU residents with more control and transparency regarding the personal data companies are collecting and using. The GDPR currently applies to companies that retain data from EU residents regardless of where the companies are located.

Kentucky has not adopted the GDPR but does have certain laws in place to protect personal information. The GDPR is focused on both informing consumers that their data is being used and including certain protections and notification procedures in the event that personal data is compromised. However, Kentucky laws on personal data are focused primarily on keeping data secure and implementing certain investigative procedures when a data breach has occurred. In other words, Kentucky’s laws, like many data laws in the United States, are centered on protecting data from a breach rather than keeping a consumer informed on how their data is being used. KRS § 61.931. They are also only applicable to government agencies or businesses who contract with government agencies. Kentucky does not currently have any data breach laws in place that apply to private businesses. The law on security and breach investigation can be found at KRS Section 61.932.

Kentucky’s notification laws are also substantially different than the GDPR requirements. The GDPR requires businesses to notify consumers within seventy-two (72) hours of discovering a breach that their data may have been compromised. However, Kentucky requires agencies to inform, at a minimum, the Kentucky State Police, the Auditor of Public Accounts, and the Attorney General within seventy-two (72) hours of discovering a breach. KRS 61.933(1). Thereafter, the agency must conduct an investigation to determine if there was a breach and whether it has or is likely to result in the misuse of personal information. *Id.* at (2). If so, the agency must notify in writing the government agencies they informed initially of a potential breach within forty-eight (48) hours of completing its investigation. *Id.* at (b)(1)(a). After the agencies have been informed, it is at that point that the investigating agency must inform any consumers that were impacted by the breach within thirty-five (35) days. *Id.* at (b)(1)(c). If no personal information has been misused and no misuse is likely to occur, then the agency has no responsibility to inform the consumers of a potential breach. *Id.* at (b)(2).