342.20 DATA PRACTICES.

Subdivision 1. **Not public data.** The following data collected, created, or maintained by the office are classified as nonpublic data, as defined by section 13.02, subdivision 9, or as private data on individuals, as defined by section 13.02, subdivision 12:

(1) application data submitted by an applicant for a cannabis business license or hemp business license, other than the data listed in subdivision 2;

(2) the identity of a complainant who has made a report concerning a license holder or an applicant that appears in inactive investigative data unless the complainant consents to the disclosure;

(3) data identifying retail or wholesale customers of a cannabis business or hemp business; and

(4) data identifying cannabis workers or hemp workers.

Subd. 2. **Public data on license applicants.** (a) The following application data submitted by an applicant for a cannabis business license or hemp business license are public data:

(1) the applicant's name and designated address;

(2) data disclosing the ownership and control of the applicant;

(3) proof of trade name registration;

(4) data showing the legal possession of the premises where the business will operate;

(5) data describing whether volatile chemicals will be used in any methods of extraction or concentration;

(6) environmental plans;

(7) the type and number of other cannabis business licenses or hemp business licenses held by the applicant; and

(8) the name, address, location, dates, and hours of where any proposed cannabis event will take place.

(b) Scoring and other data generated by the office in its review of an applicant for a cannabis business license or hemp business license are public data.

Subd. 3. **Public application data on license holders.** Once an applicant for a cannabis business license or hemp business license becomes a license holder, all of the application data that the license holder had previously submitted to the office are public data except that the following data remain classified as nonpublic data or private data on individuals:

(1) data identifying retail or wholesale customers of a cannabis business or hemp business;

(2) data identifying cannabis workers or hemp workers;

(3) tax returns, bank account statements, and other financial account information;

(4) business plans; and

(5) data classified as nonpublic data or private data on individuals by chapter 13 or other applicable law.

Subd. 4. **Civil investigative data.** Data collected or maintained by the office as part of an active investigation undertaken for the purpose of the commencement or defense of a pending civil legal action, or that are retained in anticipation of a pending civil legal action, must be subject to section 13.39.

Subd. 5. **Data practices administration.** (a) The office must establish written procedures to ensure that only individuals authorized by law may enter, update, or access data maintained by the office and classified as nonpublic or private data on individuals. An authorized individual's ability to enter, update, or access not public data must correspond to the official duties or training level of the individual and to the statutory authorization granting access for that purpose. All queries and responses, and all actions in which not public data are entered, updated, accessed, shared, or disseminated, must be recorded in a data audit trail. Data contained in the audit trail have the same classification as the underlying data tracked by the audit trail.

(b) The office must not share data classified as nonpublic or private data on individuals under this section or other data identifying an individual applicant or license holder with any federal agency, federal department, or federal entity unless specifically ordered to do so by a state or federal court.

(c) The office must arrange for an independent audit to verify compliance with this section. The audit must be completed annually for the first two years following establishment of the office and biennially thereafter. The results of the audit are public. No later than 30 days following completion of the audit, the office must provide a report summarizing the audit results to the chairs and ranking minority members of the committees and divisions of the house of representatives and the senate with jurisdiction over commerce and data practices, and the Legislative Commission on Data Practices and Personal Data Privacy. The report must be submitted as required under section 3.195, except that printed copies are not required.

History: *2023 c 63 art 1 s 20*