PRACTICE BULLETIN

Protecting Personal Information in Cannabis Purchase Transactions

On October 17, 2018, cannabis became legal in Canada. The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) applies to any private organization engaged in commercial activities that collects, uses, and discloses the personal information of individuals in Newfoundland and Labrador, including cannabis retailers. Cannabis is illegal in most jurisdictions outside of Canada. The personal information of cannabis purchasers is therefore very sensitive. For example, some countries may deny entry to individuals if they know they have purchased cannabis. While the jurisdiction of the Office of the Information and Privacy Commissioner of Newfoundland and Labrador extends only to public bodies, this guidance document's intent is to help cannabis retailers and purchasers understand their rights and obligations under *PIPEDA* and suggest best practices regarding personal information and cannabis purchase transactions.

The *PIPEDA* defines personal information as "information about an identifiable individual." This is a broad definition that can include name, date of birth, phone number, address, driver's license number, medical information, physical description, social insurance number, financial information (such as a credit card number), and more.

Collect Only What is Needed

PIPEDA limits the collection of personal information by organizations, including cannabis retailers, to the information necessary for the purposes identified by the organization. These purposes should be identified by the organization prior to the collection and the individual should be informed of those purposes at the time of collection. *PIPEDA* also requires retailers to obtain informed consent before collecting any personal information.

This means retailers need to inform individuals about what personal information is being collected and the purposes for its collection. For in-person cannabis transactions, retailers may request and review identification, such as a driver's license, to ensure the purchaser is 19 or older, but there is no need to record this information.

There may be some circumstances where a cannabis retailer is authorized to collect additional personal information. For example, a purchase made using a credit card would involve the collection of the credit card number and cardholder's name.

Video surveillance is also a form of collection and retailers must notify individuals of the surveillance with signage that is clearly visible to anyone before entering the store. That way, individuals can make an informed choice as to whether they want the retailer to collect their personal information.

Individuals seeking to purchase cannabis or cannabis products online need to be aware that the retailer is collecting their personal information (such as name, date of birth, home address,

Office of the Information and Privacy Commissioner
P.O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 or 1-877-729-6309 Fax: (709) 729-6500
E-mail: commissioner@oipc.nl.ca www.oipc.nl.ca

credit card number, purchase history, and email address). Providing personal information, especially through online formats, creates additional security risks that purchasers need to consider.

Using the Information You Collect

Retailers cannot not use the personal information they collect for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes. This means that once a transaction has been completed retailers should securely destroy the personal information collected in relation to that transaction. Similarly, retailers should develop guidelines and implement procedures to govern the destruction of personal information obtained via surveillance.

Protecting the Information You Collect

If a retailer collects personal information from purchasers, this information must be stored securely. The same applies to any personal information a retailer collects about its employees. Retailers should designate someone to be responsible for ensuring compliance with *PIPEDA*.

Retailers must protect the personal information in their custody or under their control by making reasonable security arrangements to prevent unauthorized access, collection, use, copying, modification, or disposal. This means ensuring physical, technological, and administrative security measures are in place to store personal information.

Keep in mind that storing data in the cloud or in proprietary software may involve disclosure of that personal information outside of Canada. It is preferable to store personal information on a server located in Canada to prevent access by unauthorized third parties.

Physical security measures should include:

- locking or restricting access to locations with records containing personal information; and
- using appropriate security measures such as cross-shredding documents when destroying personal information.

Technological security measures for personal information held in computer systems should include:

- using unique electronic user IDs for each staff member or purchaser;
- passwords;
- encryption and firewalls;
- restricting employee access to personal information they do not need to access to perform their job duties; and
- deleting personal information once it is no longer needed.

Administrative security measures should include:

- privacy policies;
- mandatory new and on-going staff privacy training; and
- regular risk assessments and compliance monitoring.

Advice from the Commissioner for Retailers

- Collect the least amount of personal information necessary.
- Consider collecting email addresses, but not names, for mailing lists or memberships.
- Ensure adequate physical, technological, and administrative security measures are in place to safeguard personal information.
- Designate a privacy officer.
- Create a privacy policy and train staff.
- Implement a privacy breach protocol, including the notification of the Privacy Commissioner for Canada.

Advice from the Commissioner for Purchasers

- When purchasing cannabis, do not provide the retailer with more personal information than necessary. You may need to show your identification to verify age.
- If you are concerned about using your credit card, and the option is available, consider using cash to purchase cannabis.
- If you are providing personal information to join a membership club or mailing list, consider the risks involved, and ask how your personal information will be stored.
- If you have concerns about a retailer's collection, use, storage, disclosure, or disposal of your personal information, ask to speak with their privacy officer.
- Ask retailers whether they store your personal information on servers outside of Canada. Consider only purchasing cannabis from those who keep your personal information in Canada.

PIPEDA Fair Information Principles

The 10 fair information principles that businesses must follow are:

1. Accountability;
2. Identifying Purposes;
3. Consent;
4. Limiting Collection;
5. Limiting Use, Disclosure, and Retention;
6. Accuracy;
7. Safeguards;
8. Openness;
9. Individual Access;
10. Challenging Compliance.

This document was prepared to help cannabis retailers and the public in understanding their rights and obligations under *PIPEDA* and to provide best practices in cannabis purchase transactions. This document is not intended to be relied on as legal advice and cannot be relied on as such. For the exact wording and interpretation of the *PIPEDA* please read the legislation in its entirety.