GENERAL

Updated AUGUST 2021

# Protecting personal information: Cannabis transactions

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

# PURPOSE OF THIS GUIDANCE DOCUMENT

On October 17, 2018, cannabis became legal in Canada. The *Personal Information Protection Act* (PIPA) applies to any private organization that collects, uses, and discloses the personal information of individuals in BC.

The personal information of cannabis users can be sensitive, as cannabis is illegal in most jurisdictions outside of Canada. For example, some countries may deny entry to individuals if they know the individual has purchased cannabis. This guidance document was created to help cannabis retailers and customers understand their rights and obligations under PIPA.

# PERSONAL INFORMATION

PIPA 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, image, social insurance number, financial information (such as a credit card number) and more.

# ONLY COLLECT WHAT IS NEEDED

PIPA limits the collection of personal information by organizations, including private sector cannabis retailers, to purposes that a reasonable person would consider "appropriate in the circumstances." PIPA also requires businesses to tell their customers and employees what personal information they are collecting about them, and why.

Cannabis workers may request and review identification, such as a driver's licence or BC ID card, to ensure the purchaser is 19 or older, but there is often no need to record this information. Medical information is not required to purchase non-medical cannabis or cannabis products in person or online.

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. Similarly, if a retailer distributes a newsletter or otherwise manages a mailing list, they may collect email addresses from those who sign up. They should make collecting other information, such as their customer's names, optional.

If a customer is ordering products for delivery, then the retailer must know the delivery address and the individual delivering the product will need to verify and document the purchaser's age. In some cases, customers may set up a profile for ordering via a cannabis retailer's website. Information collected and stored for this profile may include contact information (name, phone number, email), age or date of birth, credit card information, purchase history and login credentials.

## BY LAW, CANNABIS STORES MUST HAVE VIDEO SURVEILLANCE

In accordance with the Cannabis Retail Store Terms & Conditions, the Province requires cannabis retailers to have video surveillance in the interior and exterior of their store. PIPA requires retailers to give notice that an area is under video surveillance. This means that cannabis retailers must post signs in an easily viewable location to advise those entering the store about the collection of personal information via video surveillance and the purposes for collection.

## SAFEGUARDING PERSONAL INFORMATION

If a retailer collects personal information such as name, credit card number, email address, or any other personal information from purchasers, this information, including video images of an individual, must be stored securely. The same applies to any personal information a retailer collects about its employees.

**Privacy Officer**
Retailers must designate someone to be responsible for ensuring compliance with PIPA. The organization must provide that person's position name or title and contact information when requested.

**Personal Information Inventory & Classification**
It is hard for a retailer to know if they are protecting the personal information of customers and employees if they do not know what personal information they have about them. For this reason, all retailers should conduct a detailed inventory about what personal information they have about individuals and why they have it. From there, retailers can classify personal information according to sensitivity. For example, a retailer will need to take greater measures to protect their employee's SIN numbers and less for other types of personal information, such as a photo of a contest winner who has consented to having their image posted inside the retail space for promotional purposes.

**Security Measures**

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

In addition, personal information can usually only be used for the purpose for which it was originally collected and should only be kept for as long as necessary to fulfil that purpose. Once the purpose is no longer necessary for legal or business purposes, PIPA requires retailers to securely destroy that information. Retailers should formulate and implement a schedule for retention of personal information and securely destroy or remove the means by which the personal information can be associated with particular individuals in accordance with the retention schedule. Retailers should also be aware that PIPA requires organizations to keep any personal information it uses to make a decision that directly affects an individual for at least one year after using it so that they can request a copy of it. For example, if a retailer terminates an employee, they should keep the information they used to terminate the employee (such as performance reviews, customer complaints or legal opinions) for at least one year.

Some additional security controls to protect personal information include the following:

- **Physical security measures:**
    - door access monitored and recorded to areas where personal information is stored;
    - locking file cabinets and areas/offices where files are stored;
    - empty desk policies whereby all documents containing personal information are stored securely when not in use;
    - positioning computer monitors away from unauthorized personnel or customers; and
    - servers stored in a secure room and locked in cabinet.
- **Technological security measures:**
    - use of unique electronic userIDs for each staff member or customer;
    - using strong and secure passwords and changing those passwords regularly;
    - using firewalls, intrusion detection software, and antivirus software;
    - encryption, 2-factor authentication and intrusion detection and prevention systems;
    - restricting employee access to personal information they do not need to access to perform their job duties;

  - modifying equipment and software so credit card or debit numbers are removed or truncated from receipts; and
  - archiving regularly, deleting personal information once it is no longer needed and secure wiping of hard drives before discarding, selling or donating.

- **Administrative security measures:**
  - fulsome written privacy policies (see below);
  - mandatory staff training (before any new staff have access to personal information and as a regular refresher);
  - employee confidentiality agreements relating to handling personal information;
  - conducting privacy spot checks and reminding employees about protocols; and
  - conducting regular risk assessments and compliance monitoring to see if program controls need to be updated and to ensure the organization is meeting the requirements of PIPA.

For additional information about securing personal information, including storing personal information with third party providers (such as in the "cloud") please see our security self-assessment tool on our website.

**Privacy Policies**

All private organizations in BC are required by law to develop written policies and practices to meet their responsibilities under PIPA, including developing a process to respond to complaints about management of personal information. A privacy policy is critical to building trust and mitigating privacy risk.

Privacy policies are only effective when management and staff understand and are committed to following them. The best way of ensuring this is for management to emphasize that protection of personal information is a company priority and to ensure that all staff are trained in, have reviewed, understand, and follow the privacy policy in everyday transactions. Guidance on what to include in privacy policies can be found in our "Developing a Privacy Policy Under PIPA" Guidance Documents, available at this url: https://www.oipc.bc.ca/guidance-documents/2286.

Retailers who have websites, and especially those with a customer login, should have a separate privacy policy posted online that informs visitors to the webpage about the personal information collected (such as tracking cookies and website analytics) and the reasons for collection.