Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

GUIDANCE DOCUMENT | PIPA

PROTECTING PERSONAL INFORMATION: CANNABIS TRANSACTIONS

OCTOBER 2018

CONTENTS

PURPOSE OF THIS GUIDANCE DOCUMENT

On October 17, 2018, cannabis will become 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.

Cannabis is illegal in most jurisdictions outside of Canada. The personal information of cannabis users is therefore very sensitive. For example, some countries may deny entry to individuals if they know they have purchased cannabis. This guidance document was created to help cannabis retailers and purchasers 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, 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." It 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, 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 no need to record this information. Medical information or other personal information is not required to purchase cannabis or cannabis products in person.

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 offers a membership club or distributes a mailing list, they may collect email addresses for those who sign up. Retailers should consider collecting the minimum amount of personal information required for mailing lists or memberships

If a retailer is considering using video surveillance to monitor the store, it is important to note that capturing an individual's image or voice constitutes a collection of personal information. Again, PIPA requires consent before the collection of personal information. Retailers should only use video surveillance if less privacy-intrusive measures, such as hiring a security guard, are not successful. If retailers choose to use video surveillance, they must notify individuals with signage that is clearly visible to anyone before entering the store. That way, individuals can choose to shop elsewhere if they do not want the retailer to collect their personal information.

Individuals seeking to purchase cannabis or cannabis products online from retailers in other provinces also need to be aware that the retailer is collecting their personal information (such as name, date of birth, home address, credit card number, purchase history, and email address). Providing personal information, especially through online formats, creates additional security risks that purchasers need to consider.

One way to minimize the possibility of foreign disclosure, a data breach, or other incidents that reveal purchasers' names or other personal information is to not record customers' personal information.

ADVICE FROM THE COMMISSIONER FOR RETAILERS	Collect the least amount of personal information possible.
	Consider collecting email addresses, but not names, for mailing lists or memberships.
	Determine whether less privacy intrusive alternatives to video surveillance are appropriate. Only use video surveillance as a last resort.

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.

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 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.

Security Measures
Cannabis 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. In addition, personal information can 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, the personal information should be securely destroyed.

- Physical security measures include:
    - locking or restricting access to locations with records containing personal information (i.e. filing cabinets and management offices); and
    - using appropriate security measures such as cross-shredding documents when destroying personal information.

- Technological security measures for personal information held in computer systems include:
    - use of unique electronic user IDs for each staff member or purchaser;
    - passwords;
    - encryption;
    - 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 such as privacy policies and mandatory staff training (before any new staff have access to personal information and as a regular refresher) are critical components of meeting a retailer's obligations under PIPA. In addition, retailers should conduct 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.

Keep in mind that storing data in the Cloud or in proprietary software means there is likely disclosure of that personal information outside of Canada. It is much more privacy protective to store personal information on a server located in Canada to prevent access by unauthorized third parties.

Privacy Policies

Private organizations in BC are required by law to develop 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, understand, and follow the privacy policy in everyday transactions. Guidance on what to include in privacy policies can be found under "Resources" on our website: https://www.oipc.bc.ca.

Retailers who have websites, and especially those with a membership 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.

ADVICE FROM THE COMMISSIONER FOR RETAILERS	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.
	Visit www.oipc.bc.ca/resources/guidance-documents/ for guidance on how to comply with PIPA.

ADVICE FROM THE COMMISSIONER FOR PURCHASERS	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. Opt to only purchase cannabis from those who keep your personal information in Canada.