mcmillan

THE PRIVACY COMMISSIONER'S GUIDE TO PROTECTING PERSONAL INFORMATION IN CANNABIS TRANSACTIONS

Posted on January 30, 2019

Categories: Insights, Publications

The Office of the Privacy Commissioner of Canada recently released a guidance document for Canadian private sector cannabis retailers who collect personal information from their customers.

The safeguarding of personal information in the context of cannabis transactions is particularly significant since cannabis is illegal in most jurisdictions outside of Canada, which makes the collection and storage of personal information of cannabis users especially sensitive.

Collecting personal information in compliance with PIPEDA

The guidance document relates to compliance with the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA currently applies to all Canadian privacy sector cannabis retailers except those operating entirely in Quebec, Alberta or British Columbia, which have each enacted substantially similar privacy legislation.

PIPEDA defines personal information as "information about an identifiable individual," and limits the collection of personal information to that which is necessary for the purposes identified by the organization. These purposes must be in line with what a reasonable person would consider appropriate in the circumstances.

Before collecting any personal information, PIPEDA requires cannabis retailers to obtain meaningful consent. In order to obtain meaningful consent, customers need to be informed of:

1. what personal information is being collected;
2. who their personal information will be disclosed to;
3. the purposes for its collection; and
4. any risks of harm.

Given the requirements of PIPEDA, the Privacy Commissioner recommends that cannabis retailers:

- be clear on what information needs to be collected during in-person transactions, keeping in mind that requirements may differ across jurisdictions;

- be aware of any circumstances that require the collection of additional personal information (i.e. credit card transactions, distributing mailing lists, and membership programs);
- be cognisant of consent requirements when using video surveillance and determine whether less privacy intrusive alternatives are appropriate. If video surveillance is used, the retailer should notify individuals with signage that is clearly visible to anyone before entering the store;
- be proactive in making online customers aware when their personal information is collected; and
- refrain from recording personal information, where possible.

Adopting security measures to protect personal information

Cannabis retailers must store the personal information securely to prevent unauthorized access, disclosure, use, copying, or modification. The sensitivity of the information will enhance the level of protection required. For example, payment information and health information will require particularly secure protection mechanisms.

Appropriate security measures will include a combination of physical, technological, and organizational security controls. Examples of physical security measures include locking or restricting access to locations with records containing personal information and cross-shredding documents when destroying personal information. Technological security measures may include strong passwords, encryption and firewalls. Finally, organizational safeguards may include mandatory staff training and security screening of staff.

Cannabis retailers should also be particularly mindful of the risks associated with storing data in the Cloud since this may include the transfer or storage of personal information outside of Canada, which could then potentially be accessed by foreign law enforcement. When possible, storing personal information on a server located in Canada will generally be more privacy protective for cannabis retailers.

Adopting strong privacy policies

Private sector cannabis retailers are required develop effective privacy policies and practices, including a process to respond to complaints about management of personal information. These policies ensure accountability within the organization and helps to mitigate privacy risks. To ensure that such policies and practices are effectively implemented, management should conduct regular training of all staff members in privacy policies as it pertains to everyday transactions.

Retailers must also appoint a designated privacy officer who is responsible for ensuring compliance with PIPEDA. If requested, the retailer must provide that person's position name or title and contact information.

by Mitch Koczerginski, Lyndsay Wasser and Sara Ruhani, Articling Student

mcmillan

a cautionary note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.