

B.C. Privacy Commissioner Issues Guidance for Cannabis Retailers and Purchasers

The personal information of cannabis users in Canada is sensitive and can present significant risks and potential liabilities to cannabis retailers. The British Columbia Information and Privacy Commissioner has issued [guidance](#) to help cannabis retailers and purchasers understand their rights and obligations under the British Columbia *Personal Information Protection Act*. The guidance is useful for cannabis retailers and purchasers throughout Canada.

Canadian Privacy Laws

Canadian private sector personal information protection statutes – the Canadian *Personal Information Protection and Electronic Documents Act*, the Alberta *Personal Information Protection Act*, the British Columbia *Personal Information Protection Act* and the Québec *An Act respecting the Protection of Personal Information in the Private Sector* – are based on internationally recognized *Fair Information Principles*, which include: identifying purposes, consent, data minimization (limiting collect, use, disclosure and retention), safeguards and openness. Cannabis retailers in British Columbia must comply with each of the Fair Information Principles as reflected in the British Columbia *Personal Information Protection Act*.

The Guidance

On October 16, 2018, the Office of the Information and Privacy Commissioner for British Columbia issued guidance titled [Protecting Personal Information: Cannabis Transactions](#), to help private sector cannabis retailers and cannabis purchasers understand their rights and obligations under the British Columbia *Personal Information Protection Act*.

The guidance explains that cannabis users' personal information is "very sensitive", because cannabis is illegal in most jurisdictions outside Canada and some countries may deny entry to individuals if they know they have purchased cannabis. The guidance addresses a number of important issues. Following is a summary.

▪ Consent

- Cannabis retailers must obtain individuals' informed consent before collecting their personal information, which requires cannabis retailers to inform individuals about what personal information is being collected and the purposes for the collection.
- Cannabis retailers may use personal information only for the purposes for which it was originally collected.
- The purchase of cannabis products from online retailers will require the collection of personal information, which presents additional security risks that cannabis purchasers should consider.
- Cannabis purchasers concerned about using their credit card to purchase cannabis should consider using cash instead.

▪ Data Minimization

- Cannabis retailers should collect and record the minimum amount of personal information necessary for reasonable, disclosed purposes.
- Cannabis purchasers should not provide a cannabis retailer with more personal information than is necessary. For example, an individual's medical information or other similar personal information is not required to purchase cannabis products in person.

- Cannabis retailers can minimize the possibility of unintended disclosures of personal information by not recording customers' personal information. For example, a cannabis retailer might request and review an individual's government issued identification to verify the individual's age, but there is no need for the retailer to record that information.
- Cannabis retailers who offer a membership club or distribute to a mailing list may collect email addresses for individuals who sign up, but should consider not collecting individuals' names for those purposes.
- Cannabis retailers should use video surveillance only if less privacy-intrusive measures (e.g. a security guard) are not successful, and must notify individuals with clearly visible signage so they can choose to shop elsewhere if they do not want their image recorded by the surveillance system.
- Cannabis retailers should keep personal information only for as long as necessary to fulfil the purposes for which it was originally collected, and then the personal information should be securely destroyed.
- **Safeguards**
 - Cannabis retailers must securely store the personal information they collect from cannabis purchasers and the personal information of the retailers' employees.
 - Cannabis retailers must designate an individual to be their privacy officer responsible for compliance with privacy laws.
 - 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 of the information. Cannabis retailers must use physical, technological and administrative security measures to safeguard personal information. For example, unique electronic identifiers for staff and cannabis purchasers, passwords, encryption, firewalls, restricted employee access to information, and deleting personal information that is no longer needed.
 - Cannabis retailers should conduct regular risk assessments and monitoring to ensure compliance with privacy laws.
- Storing personal information in the Cloud means there is likely disclosure of the personal information outside Canada. It is more privacy protective to store personal information on a server located in Canada.
- **Identifying Purposes and Openness**
 - Cannabis retailers must develop policies and practices (including a process to respond to privacy complaints) for compliance with privacy laws.
 - An effectively implemented privacy policy is critical to building trust and mitigating privacy risk.
 - Cannabis retailers should emphasize the importance of protecting privacy, and ensure that staff are trained in, understand and follow the privacy policy in everyday transactions.
 - Cannabis retailers with websites should have a separate online privacy policy that informs website users about the personal information collected by the website (e.g. tracking cookies and website analytics) and the reasons for collection.
 - Cannabis purchasers should ask how their personal information used for a membership club or mailing list will be stored by the cannabis retailer.
 - Cannabis purchasers should ask retailers whether they store their personal information on servers outside Canada, and only purchase cannabis from retailers who store personal information in Canada.

Comment

Cannabis retailers should be mindful of the sensitivity of their customers' personal information, and should take appropriate measures to safeguard that information and protect it against unnecessary disclosures, including disclosures to third party service providers (e.g. payment service providers). Failure to protect customers' personal information might expose a cannabis retailer to significant costs and potential liabilities. For example, Health Canada's alleged unauthorized disclosure of approximately 40,000 medical marijuana users' personal information, by sending them oversized envelopes addressed to their name with a return address to the Marijuana Medical Access Program, is currently the subject of a [class action lawsuit](#) in the Federal Court of Canada.

The guidance issued by the British Columbia Information and Privacy Commissioner is generally consistent with previous guidance issued by Canadian privacy commissioners regarding the handling of personal information by private sector organizations, and may be useful for cannabis retailers and purchasers in all Canadian provinces and territories.

However, certain aspects of the guidance (e.g. comments regarding the use of cloud services to store personal information outside Canada) might be more restrictive than required for compliance with Canadian personal information protection statutes and current best practices. ■

Author

Bradley J. Freedman

T 604.640.4129

bfreedman@blg.com

BLG's Privacy/Data Protection Law Group and Cybersecurity Law Group help clients manage cyber risks, achieve legal compliance and respond to security incidents across Canada. More information is available at blg.com/privacy and blg.com/cybersecurity.

Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Ira Nishisato	Toronto	416.367.6349
Robert J. C. Deane	Vancouver	604.640.4250

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances.
Copyright © 2018 Borden Ladner Gervais LLP.

BLG Vancouver

1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com