

LIDSTONE & COMPANY  
BARRISTERS AND SOLICITORS

MEMORANDUM

**TO:** Clients  
**FROM:** Justin Leung  
**DATE:** January 30, 2023  
**RE:** *Freedom of Information and Protection of Privacy  
Amendment Act Coming into Force February 1, 2023*  
**FILE:** 99999 - 044

---

On February 1, 2023 two new sections of the *Freedom of Information and Protection of Privacy Amendment Act* Bill 22-2021(FIPPA) and regulations will come into force. The two most significant new requirements for all public bodies in BC include 1) a Privacy Management Program and 2) Privacy Breach Notifications.

**1) Privacy Management Program**

The new sections of *FIPPA* have detailed certain conditions a Privacy Management Program must meet. Public bodies are required to have a Privacy Management Program in place that includes the following:

- a) Appointing a project lead with sufficient knowledge and authority to manage the program and assess the findings. This project lead can be the Privacy Officer.
- b) Ensuring oversight by executive management through a project lead.
- c) Involving human resources, risk management, internal audit and IT personnel.
- d) Obtaining outside privacy expertise when necessary.
- e) Obtaining and documenting information to assess compliance, through staff interviews, file reviews and IT system reviews.
- f) Regularly reporting to executives on progress and implementing any resulting policies or directions from the executive.

VANCOUVER OFFICE:  
#1300 - SUN TOWER - 128 PENDER STREET WEST  
VANCOUVER, BC V6B 1R8

CALGARY OFFICE:  
BOW VALLEY SQUARE 2, #3300 - 205 5TH AVENUE, SW  
CALGARY, AB T2P 2V7

- g) Reporting to executives on any identifiable risk and compliance issues.
- h) Providing a final report of all findings to executives with a full mapping of findings against *FIPPA*'s requirements.
- i) Taking any other steps that might, considering the public body's own situation, be effective in documenting its current state of compliance and the way forward.

Privacy training should be mandatory for all employees and the training process should be documented. Public bodies are also expected to assess and revise their Privacy Management Programs on an ongoing basis.

## **2) Privacy Notification Breaches**

The new sections and regulations of *FIPPA* impose new and more stringent requirements on public bodies in the event of any privacy information breaches. This includes giving individuals notice when collecting personal information, responding to requests for access to their own personal information, individual requests for the correction of personal information and individual requests for access to records that hold someone else's personal information.

Public bodies will now also be required to report any privacy breach that "could be expected to result in significant harm to the individual". Privacy breaches include the theft, loss, or any unauthorized collection, use or disclosure of personal information. Significant harm includes identity theft, significant bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, negative impact on a credit record and damage or loss of property.

Notifications to the affected individual(s) must (1) be written and include (2) descriptions of the breach, (3) any containment steps taken, (4) contact information for a person who can provide answers on behalf of the public body and (5) steps the individual can take to reduce their risk of harm. Public bodies will also be required to provide notice of these breaches to the Office of the Information & Privacy Commissioner.

*Note: This bulletin is of a general and summary nature and is not exhaustive of all possible legal obligations. Laws may change over time and should be interpreted only in the context of particular circumstances such that these materials are not intended to be relied upon or taken as legal advice or opinion. Readers should consult a legal professional for specific advice in any particular situation.*