Bulletin | Cybersecurity, Privacy and Data Protection

December 2022

New privacy compliance requirements coming under B.C.'s FIPPA legislation

Commencing February 1, 2023, British Columbia's public sector privacy statute – the *Freedom of Information and Protection of Privacy Act* – will require public bodies to have a privacy management program and to comply with privacy breach notification obligations. Accordingly, public bodies should now prepare for compliance with those new requirements.

Introduction

British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA) regulates how provincial public bodies in British Columbia (e.g., provincial government ministries and agencies, municipalities, crown corporations, post-secondary institutions, school boards, health authorities and self-governing bodies of professions) collect, use, disclose and retain personal information. FIPPA also provides access rights to certain records and personal information held by public bodies in British Columbia and establishes a regime of independent review and oversight.

In November 2021, the Government of British Columbia enacted Bill 22, *Freedom of Information and Protection of Privacy Amendment Act, 2021* (Bill 22) to make significant amendments to FIPPA, including new requirements for privacy management programs and privacy breach notification obligations that come into force on a date set by regulation. See BLG bulletin *Changes to B.C.'s public sector privacy legislation*.

In November 2022, the Government of British Columbia approved Order in Council No. 638, which provides that the requirements for privacy management programs and privacy breach notification obligations will come into force on February 1, 2023.

Privacy management programs

Commencing February 1, 2023, FIPPA (as amended by Bill 22) will require the head of a public body to develop a privacy management program that complies with directions of the Minister of Citizens' Services. *Ministerial Direction 02-2022, Privacy Management Program Direction* (the Direction), effective February 1, 2023, provides public bodies with a framework that outlines required components of a privacy management program. The Direction explains that privacy management programs "are vital to ensuring

public bodies are accountable and transparent with respect to their management of personal information" and "promote trust by assuring information sharing partners and the public that the public body is protecting the personal information in its custody or under its control".

The Direction details seven components that must be included in a privacy management program and explains that the components "should be reasonable and scaled commensurate with the volume and sensitivity of the personal information in the public body's custody or under its control". The required components are as follows:

1. The designation, by the head of a public body, of one or more individuals to be responsible for: (a) being a point of contact for privacy-related matters, such as privacy questions or concerns; (b) supporting the development, implementation and maintenance of privacy policies and procedures; and (c) supporting the public body's compliance with FIPPA.
2. A process for completing and documenting privacy impact assessments as required and information-sharing agreements as appropriate under FIPPA.
3. A documented process for responding to privacy complaints and privacy breaches.
4. Privacy awareness and education activities, undertaken at timely and reasonable intervals, to ensure employees are aware of their privacy obligations.
5. Privacy policies and documented privacy processes or practices available to employees and, where practicable, to the public.
6. Methods to ensure that service providers are informed of their privacy obligations.
7. A process for regularly monitoring and updating the privacy management program to ensure it remains appropriate to the public body's activities and is compliant with FIPPA.

Privacy breach notification obligations

Commencing February 1, 2023, FIPPA (as amended by Bill 22) will require the head of a public body to give notice to affected individuals and the Information and Privacy Commissioner of British Columbia (the Commissioner) of privacy breaches affecting personal information in the custody or under the control of the public body, which includes personal information processed by a service provider on behalf of the public body. The new privacy breach notification obligations are generally consistent with similar obligations under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and other provincial private sector privacy laws. See BLG bulletin *Frequently Asked Questions – Compliance with PIPEDA's Security Breach Obligations*.

Details of the breach notification obligations are set out in FIPPA (as amended by Bill 22) and in amendments to The *Freedom of Information and Protection of Privacy Regulation, B.C. Reg. 155/2012*. Following is a summary:

- FIPPA broadly defines "privacy breach" as the theft or loss, or unauthorized collection, use or disclosure, of personal information in the custody or under the control of a public body.
- The head of a public body must notify affected individuals and the Commissioner in a prescribed manner and "without unreasonable delay" if a privacy breach involving personal information in the custody or under the control of the public body "could reasonably be expected to result in significant harm" to an individual.
- FIPPA broadly defines "significant harm" as including identity theft, significant bodily harm, significant humiliation, significant damage to reputation or relationships, significant loss of employment, business or professional opportunities, significant financial loss, significant negative impact on a credit record, and significant damage to, or loss of, property.
- There are limited exceptions to the obligation to notify affected individuals.
- Privacy breach notifications to affected individuals must usually be given in writing directly to each individual and must include prescribed information about the privacy breach. Indirect privacy breach notifications to affected individuals are permitted in limited circumstances, provided that an indirect notification is given by public communication that can reasonably be expected to reach the affected individual and contains the prescribed information.
- A privacy breach notification to the Commissioner must be given in writing and must include prescribed information about the privacy breach.

The privacy breach notification obligations imposed on the head of a public body are supported by a FIPPA requirement that an employee, officer or director of a public body, or an employee or associate of a service provider, who knows that there has been an unauthorized disclosure of personal information in the custody or under the control of the public body must immediately notify the head of the public body. FIPPA provides that failure to notify the head of the public body of an unauthorized disclosure of personal information is an offence punishable on conviction by fines of up to $50,000 for individuals and up to $500,000 for corporations.

Comment

Public bodies in British Columbia should now prepare for compliance with FIPPA's new privacy management program requirements and privacy breach notification obligations.

To prepare for compliance with FIPPA's new requirement for a privacy management program, public bodies should review their current privacy management policies, procedures and practices and make changes required for compliance with the Direction. BLG bulletin *2022 Privacy risk management – Top tips for organizations* provides five top tips and a checklist to help organizations improve their privacy practices.

There are several steps that public bodies should take to prepare for compliance with FIPPA's new privacy breach notification obligations, including:

- Assess existing security safeguards for personal information, and consider whether additional or enhanced safeguards will reduce the risk that a privacy breach will occur or will result in significant harm to individuals.
- Establish written policies and procedures so that each privacy breach is promptly escalated to properly trained personnel for response in accordance with a suitable written incident response plan. Periodically test and improve the plan.
- Establish a written framework for assessing whether a privacy breach could reasonably be expected to result in significant harm, so that trained personnel (with the benefit of appropriate legal advice) make and document consistent decisions about giving notice of privacy breaches to affected individuals and the Commissioner.
- Establish written guidelines for determining how notice of a privacy breach should be given to affected individuals and whether limited exceptions to the notification obligations are applicable.
- Establish a legal privilege strategy to help avoid inadvertent and unnecessary disclosure of confidential legal advice.
- Ensure that contracts with service providers contain appropriate provisions to support the public body's compliance with privacy breach notification obligations. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Danielle Windt
T 604.640.4120
dwindt@blg.com

BLG's national Compliance with Privacy and Data Protection group includes lawyers, located in BLG's offices across Canada, with expertise in Canadian and international privacy laws, cyber risk management and class action litigation. We provide both proactive compliance advice and legal advice to help respond to a privacy breach or resolve privacy disputes. Additional information about BLG's national Compliance with Privacy and Data Protection group and our services is **available here**.