Bulletin | Cybersecurity, Privacy and Data Protection

January 2022

Changes to B.C.'s public sector privacy legislation

In November 2021, the Government of British Columbia enacted Bill 22 to make significant changes to the *Freedom of Information and Protection of Privacy Act*, which governs how public bodies in British Columbia collect, use, disclose and retain personal information. Some changes present new opportunities, while other changes impose new obligations and potential liabilities. Public bodies and their service providers should take steps for compliance with the legislative changes.

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. In 2016, a *Special Committee* issued a *report* with recommendations for changes to FIPPA, but those recommendations were not implemented.

Bill 22, Freedom of Information and Protection of Privacy Amendment Act, 2021 ("**Bill 22**"), most of which came into force on November 25, 2021, made significant changes to FIPPA, including modifications to FIPPA's data residency requirements, new privacy breach notification obligations, requirements for privacy management programs and new privacy offences. When introducing Bill 22, the Government explained: "These amendments help people continue to access the services they need faster, while ensuring their privacy is protected. We're making changes today to keep pace with advancements in technology and provide the level of service that people expect in the digital era".

Bill 22 provides that further details and requirements regarding certain amendments will be set out in regulations and ministerial directions. As of the date of this bulletin, the only new regulations/directions are *Personal Information Disclosure for Storage Outside of Canada Regulation*, *Ministerial Direction 1-21, Privacy Impact Assessment Directions (Ministries)*, and *Ministerial Direction 2-21, Privacy Impact Assessment Directions (Non-Ministries)*.

Summary of key changes

Following is a summary of some of Bill 22's key changes to FIPPA's personal information protection provisions.

Data residency

Bill 22 significantly changed FIPPA's strict rules regarding data residency. Previously, FIPPA prohibited public bodies and their service providers (including cloud service providers) from disclosing, storing or permitting access to personal information outside Canada except in limited circumstances. As a result of Bill 22, public bodies may now disclose personal information outside Canada provided they comply with applicable regulations. The Ministry of Citizens' Services explained that the changes to the data residency requirements "help public bodies keep pace with new technology and provide the services people expect in a modern age".

As of the date of this bulletin, the only relevant regulation is the *Personal Information Disclosure for Storage Outside of Canada Regulation*, which requires the head of a public body to conduct a prescribed privacy impact assessment of each new program, project and system in which "sensitive" personal information is "disclosed to be stored outside of Canada". Prescribed requirements for privacy impact assessments are set out in *Ministerial Direction 1-21, Privacy Impact Assessment Directions (Ministries)*, and *Ministerial Direction 2-21, Privacy Impact Assessment Directions (Non-Ministries)*. The requirement for a privacy impact assessment does not apply to programs, projects or systems in existence as of November 26, 2021 or if the information is made available to the public under an enactment that authorizes or requires it to be made public.

The new Regulation does not identify or limit the kinds of personal information considered "sensitive" or explain whether a privacy impact assessment will be required when personal information is transferred outside of Canada for processing but not for storage. However, those issues might be addressed by future regulations or regulatory guidance.

Privacy breach notification obligations

Bill 22 added to FIPPA new privacy breach notification obligations that align with similar obligations under the public sector privacy laws of other provinces. The new notification obligations are not in force as of the date of this bulletin.

Previously, FIPPA did not require public bodies to give notice of a privacy breach to affected individuals or the Information and Privacy Commissioner of British Columbia (the "**Commissioner**"). As a result of Bill 22, public bodies that suffer a "privacy breach" (broadly defined as theft or loss, or the unauthorized collection, use or disclosure, of personal information in the custody or control of a public body) must, without unreasonable delay, notify affected individuals and the Commissioner if the privacy breach "could reasonably be expected to result in significant harm to the individual". "Significant harm" is broadly defined and includes identity theft, significant humiliation, significant damage to reputation or relationships, significant loss of employment, business or professional opportunities, significant financial loss, and significant negative impact on a credit record. There are limited exceptions to the obligation to notify affected individuals.

Notifications to affected individuals and the Commissioner must be made in a manner prescribed by regulations, but the regulations have not been published as of the date of this bulletin. The Commissioner previously issued guidance for responding to and giving notices of a privacy breach: *Privacy Breaches: Tools and Resources*.

Privacy management programs

Bill 22 amends FIPPA to require the head of a public body to develop a privacy management program that complies with directions of the Minister of Citizens' Services. As of the date of this bulletin, the amendment is not in force and the Minster has not issued directions. However, the Commissioner and the Minister of Citizens' Services previously issued guidance for establishing and implementing a privacy management program: *Accountable Privacy Management in BC's Public Sector* and *Privacy Management and Accountability Policy*.

New privacy offences

Bill 22 added new privacy offences to FIPPA, including offences relating to the unauthorized collection, use or disclosure of personal information and a failure to report an unauthorized disclosure of personal information. The amendments provide that a public body's service provider commits a privacy offence if any of its employees or associates commit the privacy offence. In addition, the amendments provide that a corporate officer, director or agent who authorizes, permits or acquiesces in the commission of a privacy offence by their corporation also commits an offence. A person convicted of committing a new privacy offence is liable to a fine of up to $50,000 for individuals and up to $500,000 for corporations. There is a due diligence defence for service providers and their employees and associates.

Comment

Some aspects of Bill 22 are controversial. The Commissioner has commented that while some of the amendments to FIPPA are welcome, "several of [the amendments] are of deep concern". For more information, see October 20, 2021 letter to Minister of Citizens' Services and October 18, 2021 statement of the Commissioner.

The full effect of Bill 22 on the personal information practices of public bodies and their service providers will not be known until the Government of British Columbia issues additional regulations and ministerial directions. Nevertheless, public bodies should now take steps for compliance with the new FIPPA provisions, including:

- **Data residency:** Establish internal policies and procedures (including provisions for contracts with service providers) for processing and storing personal information outside Canada. Prepare to conduct appropriate privacy impact assessments for new programs, projects and systems that will store (and possibly process) personal information outside Canada. Consider required changes to privacy policies/notices.
- **Privacy breach notification:** Review and revise privacy breach response plans to include guidance for compliance with breach notification obligations. Ensure relevant personnel are appropriately trained and have access to required legal advice. Consider required provisions for contracts with service providers.
- **Privacy management programs:** Review current privacy management programs (including service provider risk management) and prepare to revise the programs to comply with ministerial directions.
- **Privacy offences:** Educate relevant personnel about the new privacy offences. Consider required provisions for contracts with service providers.

Service providers to public bodies should also take steps for compliance with the new FIPPA provisions, including implementing policies and procedures required to support a due diligence defence to potential privacy offences. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Allison Foord
T 604.640.4079
afoord@blg.com

Katherine M. Stanger
T 604.640.4150
kstanger@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**.