YOUNG ANDERSON
BARRISTERS & SOLICITORS

November 30, 2021

BULLETIN

UPDATE ON SIGNIFICANT AMENDMENTS TO THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Significant changes to British Columbia's freedom of information and privacy law came into force on November 25, 2021.

As our previous bulletin on Bill 22 discusses in more detail, the amendments to the *Freedom of Information and Protection of Privacy Act* (FIPPA) include these significant changes:

- a duty to adopt a privacy management program,
- a duty to notify affected individuals and the Office of the Information and Privacy Commissioner (OIPC) of certain privacy breaches,
- enhanced privacy impact assessment requirements,
- repeal of the in-Canada data residency rule,
- a new mandatory exemption to protect certain rights and interests of Indigenous peoples,
- exclusion of some kinds of records from access requests,
- introduction by regulation of a new fee for making an access request, and
- new offence provisions.

All the amendments are now in force except for the first two listed above—along with an amendment adding two named police association organizations as public bodies—all of which will come into force later by regulation.

This bulletin draws your attention to three changes and recommends that you start working on the last two now.

Data Residency Regulations Have Been Issued

Until last week, the default under Part 3 of FIPPA was that public bodies were, with some exceptions, required to store personal information only in Canada. Last week's amendments got rid of this core rule, but there are now some important nuances established by regulation.

Public bodies can now disclose personal information outside Canada but may do so only in accordance with ministerial regulations (section 33.1(1)). The regulations were created on November 26 by Ministerial Order M462/2021.

For any future program, project, or system, a public body must conduct a privacy impact assessment (PIA) under section 69 of FIPPA and in doing so "make an assessment" respecting "each of the public body's programs, projects and systems in which personal information that is sensitive is disclosed to be stored outside of Canada." (This requirement does do not apply to a "program, project or system" already in existence on November 26.)

On the face of it, this requires a PIA only where "sensitive" personal information is involved, and then only where sensitive personal information is to be "stored" outside Canada. Even sensitive personal information can be disclosed if it does not involve storage.

It remains to be seen how the OIPC will decide if a given instance of disclosure involves storage of personal information. The OIPC could conceivably conclude that information is not "stored" outside Canada if it is only incidentally stored outside Canada, and temporarily so, to the extent necessary to perform other functions, directly or through a service provider. As we discuss later, however, we believe the OIPC is likely to expect public bodies to assess the risk, through a PIA, of even temporary, incidental storage outside Canada.

It is also clear from the regulations that FIPPA's only stricture on disclosure of personal information outside Canada relates to "sensitive" personal information. Disclosure outside Canada of personal information that is not "sensitive" is, strictly speaking, free of any express controls under FIPPA, but below we urge caution about the OIPC's likely expectations.

As for what is "sensitive" personal information, neither FIPPA nor the regulations define that term. What kinds of information might be seen as sensitive? The categories are obviously not closed, but personal health information is undoubtedly sensitive. Information about sexual orientation, gender identity, religious or political beliefs, and race or ethnicity, also are widely accepted as being "sensitive". Information revealing someone's criminal convictions, arrests, and other law enforcement records is often regarded as sensitive.

It is worth remembering here that many of these kinds of information, including personal health information, can be found in unexpected places. Personal health information, for example, is often found in human resources files or occupational health and safety files. This means that any proposal to store human resources data outside Canada will likely involve an assessment under the regulations before it can be done lawfully.

It is also important to remember that context matters. Information that might not seem truly sensitive in the domestic context can be highly sensitive if disclosed and accessed outside of Canada. An example is an employment record for someone who worked in a program supporting people experiencing discrimination because of their gender identification. This kind of

information around work history might not immediately spring to mind as "sensitive" personal information. However, there are parts of the world where this information would be sensitive, and its disclosure could potentially create risks for employees who travel to these locations.

Even though the regulations are narrowly focused on sensitive personal information, we urge caution. It is doubtful that the OIPC will treat the regulations as entirely absolving public bodies of the need to assess and mitigate risk where personal information that is *not* sensitive is to be disclosed outside the country. This may be true for non-sensitive personal information accessed outside of Canada, and very likely to be true for non-sensitive personal information stored outside of Canada. The OIPC is unlikely, we think, to overlook public bodies' duty under FIPPA to "protect" personal information using "reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal" (section 30). We believe the OIPC will expect public bodies to assess risk in relation to disclosure outside Canada of *any* type of personal information, whether "sensitive" or not.

In making this prediction, we have in mind not only the "reasonable security arrangements" duty, but also the duty to conduct a PIA for any current or proposed enactment, system, project, program, or activity. That duty has long existed in FIPPA itself and continues to exist after these amendments, with the external storage assessment required under the new regulations merely adding a gloss to that duty.

The amendments have made it even clearer that local governments must conduct PIAs, and that they must do so in accordance with ministerial directions for PIAs (section 69(5.3)). FIPPA defines the term "privacy impact assessment" as an assessment "to determine if a current or proposed enactment, system, project, program or activity meets or will meet the [privacy] requirements of Part 3" of FIPPA (section 69(1)). FIPPA also now authorizes the ministerial directions to include "different directions for different categories of personal information" (section 69(10)).

Before turning to the new PIA requirements, we should note that new data residency regulations do not apply where the information "is made available to the public under an enactment that authorizes or requires the information to be made public" (section 32(2)(f)). Again, however, the OIPC's expectations may be higher in light of the relevance of the "reasonable security arrangements" duty for all PIAs.

New PIA Directions

The PIA directions were also issued on November 26, ministerial direction 2/21. These have significant implications for when and how a PIA is conducted, implications that go beyond the issue of storage of personal information outside Canada.

The direction clarifies that a public body "must" conduct a PIA "on a new initiative for which no PIA has previously been conducted" but, importantly, that a public body must also conduct a PIA "before implementing a significant change to an existing initiative, including but not limited to a

change to the location in which sensitive personal information is stored, when it is stored outside of Canada."

The new PIA direction states that local public bodies are not required to use the provincial government's PIA template, but whatever format a PIA takes, it must assess a range of factors. Among other things, it must "identify privacy risks and privacy risk responses that are proportionate to the identified risk". Another requirement is to identify "reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or storage that have been or will be made."

If the initiative might involve storage outside Canada, the public body must also assess whether the initiative "involves personal information that is sensitive" and whether it is to be "disclosed to be stored outside of Canada". If so, the PIA must identify the privacy risks—the direction defines "privacy risk"—and identify "the level of the privacy risk(s) associated with the disclosure by examining factors", including risks such as the likelihood of unauthorized collection, the impact to individuals, whether the personal information is stored by a service provider, and where the personal information is stored.

Public bodies must then, for each "privacy risk", identify a privacy risk response that is proportionate to the level of risk posed, including "technical, security, administrative or contractual measures". The overall outcome expected "will be a risk-based decision made by the head of the public body on whether to proceed with the initiative".

We recommend that local governments familiarize themselves with the substantial changes to PIA requirements generally, not just for storage outside Canada, and implement any necessary process and policy changes to meet these new obligations.

Beginning Work on Your Privacy Breach Notification Framework

Similarly, although the privacy breach notification rules are not in force, we recommend starting to work on policies and procedures for breach notification, to be ready when these rules come into force. The OIPC's 2012 guidance on notification can help with procedures and help with how to assess risk, although it should be noted that the guidance does not take into account the legislative test for "significant harm" established by the new section 36.3 of FIPPA.

Starting to Frame Up Your Privacy Management Program

We also suggest that local governments start thinking in general terms about their privacy management program. The 2013 OIPC document on this topic offers high-level guidance on what these programs involve, though we note that ministerial regulations will be made that will have to be followed in designing programs once this provision is in force.

Our November 26, 2021, firm seminar paper on freedom of information and privacy discusses Bill 22 further, and we will provide updates as these changes begin to be put into practice.

Significant Revamping of Provincial Government Privacy Guidance Materials

In addition to the changes that we have outlined generally here, the provincial government has just published considerably revised general privacy compliance guidance materials for public bodies. These are aimed largely at government ministries, but include materials that will be helpful to local governments, including guidance on conducting PIAs in light of the changes described above. The updated materials can be found through Privacy and Personal Information in the Public Sector.

If you have any questions, please call David Loukidelis or James Barth.

David Loukidelis & James Barth