YOUNG ANDERSON
BARRISTERS & SOLICITORS

March 27, 2020

BULLETIN

PROVINCE ALLOWS DISCLOSURE OF PERSONAL INFORMATION OUTSIDE CANADA SO LOCAL GOVERNMENTS CAN CONTINUE OPERATIONS DURING THE COVID-19 PANDEMIC EMERGENCY

Local governments can now temporarily use remote working tools such as video conferencing services to help maintain their operations during the COVID-19 pandemic emergency.

The *Freedom of Information and Protection of Privacy Act* (FIPPA) prohibits storage or disclosure of any personal information outside Canada, though there are some exceptions. Ministerial Order M085, made March 26, 2020, creates another—very welcome—exception. It temporarily allows local governments (and other public bodies) to use third-party tools and applications, such as video-conferencing apps or instant messaging, while sharing or disclosing personal information of employees or other individuals.

This order supports continued local government operations where staff and elected officials are working remotely but need to carry on business. It also enables municipal councils and regional district boards to hold meetings using video conferencing and any other "third-party tool and applications" (which is defined to *include* "any software developed and maintained by a third party and which is used to enable communication or collaboration between individuals").

It is important to note that the order imposes several requirements. A key point is that personal information may be disclosed inside or outside of Canada through a third-party tool or application only if all three of these requirements are met:

1. The tools or applications are being used to support and maintain the operation of programs or activities of the public body;
2. The tools or applications support public health recommendations or requirements related to minimizing transmission of COVID-19 (such as social distancing or working from home guidance or requirements); and
3. Any disclosure of personal information is limited to the minimum amount reasonably necessary for the performance of duties by an employee, officer, or minister of the public body.

Further, the public body's FIPPA "head" must first be satisfied that a particular third-party tool or application is reasonably secure, in compliance with section 30 of FIPPA, and the public body makes all reasonable efforts to remove personal information which is collected, used or disclosed using a third party application.

Local governments will therefore need to have their IT professionals assess the information security features of each tool or application, and a preference for well-established and reputable third-party solutions would be prudent.

Local governments should also keep in mind their FIPPA duty to implement reasonable security measures to protect personal information against unauthorized access, disclosure, use or destruction continues to apply. This duty applies where, for example, employees wish to take personal information home on laptops or other portable storage devices, with encryption and other security measures being necessary.

BC's Information and Privacy Commissioner has recently issued "Tips for public bodies and organizations setting up remote workspaces", which contains links to other resources. The guidance is here: https://www.oipc.bc.ca/guidance-documents/2398

The Ministerial Order is here: http://www.bclaws.ca/civix/document/id/mo/mo/2020_m085.
Ministerial Order M083, dealing with local government meetings, is here: http://www.bclaws.ca/civix/document/id/mo/mo/2020_m083

For any questions on this matter or other privacy challenges please do not hesitate to contact David Loukidelis or Ethan Plato directly.

David Loukidelis & Ethan Plato