# New *Access to Information and Protection of Privacy Act* Will Place Obligations on Communities

Sandra MacKenzie and Lyndon Stanzell, Lawson Lundell LLP

In the NWT, the *Access to Information and Protection of Privacy Act*, or ATIPP, governs access to public records and how public bodies handle personal information. In 2019, a new version of ATIPP received assent, though it has not yet come into force. Perhaps the biggest change in the revised legislation is that it will apply to local governments, which will begin to assume obligations under ATIPP as they are added to the regulations. This staged approach will likely take place over the course of several years to give communities time to prepare. With the coming implementation of the new Act, it is important for communities to understand what their statutory obligations will be regarding access to public records and the handling of personal information.

ATIPP serves two primary purposes. Firstly, it provides for public access to public records in the hands of public bodies. The "public bodies" regulated by ATIPP include offices of the GNWT as well as other public organizations designated in the regulations, which will soon include local governments. A "record" is broadly defined as information in any form and can include adopted budgets, municipal plans, or auditor's reports. ATIPP's second purpose is protecting personal information by regulating how that information is collected and handled by public bodies. "Personal information" means information about an identifiable individual and can include names, addresses, or employment histories.

The right to access records and information, including limitations on that right, is dealt with in part one of ATIPP. Requests for records must be submitted in writing and the public body receiving the request must keep the identity of the applicant confidential. The public body has an obligation to respond to an applicant openly, accurately, and completely within 20 business days after receiving a request. It is possible to extend the deadline if a public body needs more time to properly respond to an ATIPP request.

A public body responding to an ATIPP request may disclose the record, refuse to disclose the record, or neither confirm nor deny the existence of the record. Failure by a public body to respond to an ATIPP request within the time limit will be considered a refusal of the request. If a

public body receives a request that should have gone to another public body, they have 10 days to transfer the request to the proper organization.

A public body may ask the Information and Privacy Commissioner, or IPC, for permission to disregard a request if the request is considered frivolous or made in bad faith. The IPC is an individual empowered to oversee the Act and has the power to review decisions made by public bodies with respect to ATIPP requests. Under the new Act, the IPC will be able to order a public body to take a particular course of action following a review, whereas the old ATIPP only allowed the IPC to make recommendations.

Public bodies are prohibited from disclosing information in certain situations, such as where the information would reveal the trade secrets of a third party or where the disclosure would constitute an unreasonable invasion of someone's privacy. The revised ATIPP will set out how to determine what does and does not constitute an unreasonable invasion of privacy. Public bodies also have the discretion to refuse access to public records in some situations, such as where the records are subject to solicitor-client privilege or where the disclosure might interfere with a law enforcement matter.

Part two of ATIPP deals with the protection of privacy and specifies how and when personal information may be collected, used, and disclosed. ATIPP requires public bodies to take adequate security measures to protect personal information and also provides individuals with the right to request corrections to their personal information held by a public body. The revised ATIPP will require privacy impact assessments to be completed by public bodies whenever a proposed enactment, system, project, program, or service is being developed that involves the collection, use, or disclosure of personal information. Whenever a material data breach occurs it must be reported to the IPC. If the breach presents a real and significant risk of harm to the individuals whose information is involved, those individuals must also be notified as soon as reasonably possible.

Key to properly understanding ATIPP is an awareness that the Act has many exceptions. The definitions of "records", "personal information", and "public bodies" all have exceptions that limit the application of the Act. For instance, the revised ATIPP will generally not apply to personal or constituency records of a member of a municipal council. Many of the obligations set out in the Act also have exceptions. For example, local governments will not be able to disclose confidential information if it may reveal draft resolutions or bylaws or the content of certain

municipal council deliberations. It would be good practice to regularly consult the new version of the Act once it is implemented to confirm if there are applicable exceptions in a given set of circumstances.

The new version of ATIPP will also contain a general obligation for public bodies to disclose information about a risk of significant harm to the environment or to the health or safety of the public, even absent a request. Public bodies will also be obligated to disclose information where its disclosure is clearly in the public interest for any other reason, notwithstanding anything else in the Act. Another new feature will be the requirement for public bodies to designate a coordinator to handle ATIPP requests and submit annual ATIPP reports to the Minister.

This has been a very brief overview of the framework provided by ATIPP for handling public access to records and protecting personal information as well as the incoming changes to the Act. As the revised legislation is rolled out, communities will need to develop good practices for the management of information and privacy, so it would be a good idea to begin preparing now. The following are some practical tips to consider in preparation for the new legislation:

1) Develop consistent methods and forms to be used for processing ATIPP requests. Developing a system for receiving and processing ATIPP requests based on standardized request forms can help with efficiency and streamlining.
2) Review existing forms and information collection practices. Existing forms and information collection practices should be reviewed to determine how they may engage ATIPP and if they trigger any obligations for the local government. Only the minimum amount of personal information necessary should be collected when needed.
3) Take advantage of training opportunities shared by organizations like LGANT and the GNWT Department of Municipal and Community Affairs. Organizations like LGANT and MACA can offer information on how to prepare and develop a system for managing ATIPP requests and obligations.

We hope that this general overview is helpful. This is not meant to be legal advice. If you have specific questions about ATIPP or its applications to local governments, please reach out to Sandra MacKenzie at Lawson Lundell at smackenzie@lawsonlundell.com.