OIPC Audit and Compliance Program

The Office of the Information and Privacy Commissioner for Newfoundland and Labrador (OIPC) has established an Audit and Compliance Program to assess the extent to which public bodies are protecting personal information and complying with access provisions under the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*).

A public body being reviewed under the Audit and Compliance Program may be assessed on any aspect of its *ATIPPA, 2015* obligations with regard to access, collection, use, disclosure, protection, retention, or disposal of personal information. Audits may comprise investigation, audit, research or any combination of monitoring and compliance functions. Completed audits will be published for their value as an education tool for all public bodies.

What is an Audit?

An audit provides an assessment of whether a public body is following good personal information protection practice. Audits are systematic and independent examinations that determine whether activities involving the processing of personal information are carried out in accordance with the *ATIPPA, 2015*. In meeting legislative obligations, public bodies may use a variety of tools that the OIPC may examine, including, but not limited to contracts and agreements, Privacy Impact Assessments, policies and procedures, privacy notices and privacy training for staff and end users.

An audit may focus on a particular area, function or division, such as the personal information handling practices of the Human Resource Division as a whole. It may also focus on a process, for example the personal information handling practices surrounding the recruitment process.

The Audit and Compliance Program will conduct fair and objective audits of a public body to determine how well it complies with obligations under *ATIPPA, 2015*. The audit may examine:

- whether it maintains adequate administrative, physical and technological safeguards to protect personal information from unauthorized access, collection, use, disclosure, disposal or similar risks; and
- the extent to which it has established and maintains adequate procedures for managing requests for information.

The purpose of the Audit and Compliance Program is to provide a mechanism to:

- enhance oversight regarding the management of personal information across NL public bodies;
- measure the level of compliance of public bodies with provincial privacy and access laws; and
- make recommendations, where needed, to improve privacy and access practices, policies, guidelines, and laws.

Audits

Audits will identify areas where a public body may excel with regard to compliance, safeguards, and overall access or privacy management. They will also highlight, importantly, areas where improvements are needed in order to comply with legislation and guidelines.

There are many aspects of access or privacy that can be assessed to determine the extent to which public bodies are protecting personal information and complying with access provisions of applicable legislation. Some examples include:

Management, Policies and Procedures

Reviewing a public body's management of access to information and protection of privacy programs; access to information and privacy policies and procedures; and information and data sharing agreements.

Collection, Use, Disclosure and Retention

Assessing the collection, use, disclosure and retention of personal information by the public body; whether appropriate notice and consent has been obtained; and whether the public body limits collection, use, disclosure and retention of personal information to only what is needed to administer a program or business.

Protections and Safeguards

Examining a public body's access, disclosure or protection provisions; administrative, technical and physical safeguards; staff knowledge and training related to privacy and the protection of personal information; and whether and how a public body protects personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Access Processes

Reviewing a public body's access to information processes; how it handles access-related requests or complaints; timelines for responding to access requests; and compliance with other access-related obligations under the *ATIPPA, 2015*.

Accountability and Compliance Monitoring

Evaluating how the public body monitors compliance with its privacy policies and procedures; accountability practices; how it handles privacy-related complaints; whether it conducts internal or external audits of safeguards; and whether it analyzes breaches that may have occurred.

Benefits of Audits

Audits, be they internal or external, offer many benefits. Legislative requirements apply, even if a public body is not aware of its obligations.

Benefits of audits include:

- Confirmation of the legal authority to collect, use, retain and disclose personal information.
- The ability to demonstrate due diligence and evidence of compliance needed to support informed decision-making. This information may also be important in the event of a privacy breach or complaint to the Information and Privacy Commissioner.

- The reassurance of individuals, other institutions, partners and internal management that best practices are being followed. Audits may even encourage the development of a privacy culture within the public body.
- Improvement of transparency and better individual awareness, understanding and trust of of the public body's information management practices.
- Improvement of operational efficiencies.

Limitations of Audits

It is important to keep in mind that any audit will be limited in its applicability by its scope and objectives; the period of time captured in fieldwork; the specific areas of the public body that were assessed; the availability of applicable information; and the margin of error. Such details may limit the generalizability of audit findings across the public body, other time periods, and other similar public bodies.

As such, the final report should not be seen as a definitive account of a public body's total personal information handling practices; nor should the report be seen as an endorsement of the public body's compliance with its obligations under the *ATIPPA, 2015*.

Audit Criteria

The OIPC has adopted the Generally Accepted Privacy Principles (GAPP) that form the foundation for the Privacy Maturity Model developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) as the standard against which audits will occur.

Key Legislative Authority and Powers

The Commissioner's general powers and duties are established in section 95 of the *ATIPPA, 2015*. The Commissioner may, among other powers and duties:

- conduct investigations to ensure compliance with the Act;
- monitor and audit the practices and procedures used by public bodies to carry out the responsibilities placed on them by the Act;
- consult with anyone with experience or expertise in any matters related to the purpose of the Act; and
- engage in or commission research relating to the purpose of the Act.

With respect to audit and compliance specifically, the Commissioner has the authority to:

- monitor and audit (section 95);
- compel the production of documents (section 97);
- enter the premises of a public body and to interview staff (section 98); and
- delegate his duties and powers to any person (section 103).

There are also general restrictions on disclosure by the Commissioner and OIPC staff (section 102) that provide certain protections to individuals who have made statements or answered questions during an audit by the OIPC.

Identifying an Entity or Program for Audit

As the OIPC NL is not able to audit every public body on an ongoing basis, the following guidance has been developed to assist in identifying the most effective use of audit resources. In general, the OIPC NL will consider the number of individuals potentially affected, the nature and sensitivity of the personal information being processed, and the nature and extent of any likely damage or distress caused by non-compliance when identifying subjects and entities for audit.

The OIPC NL will select topics or entities to assess based on a variety of factors and resources, including:

- complaints received;
- breach reports received;
- business intelligence;
- follow-up;
- general communications;
- legislative authority.

In general, once identified for audit, the public body is informed of the audit subject and the reasons it was selected for audit.

Take Action Now

To ensure compliance with the *ATIPPA, 2015*, every public body must determine the current state of its personal information holdings and related procedures. Each public body needs to know what it has in the way of personal information, where it is stored and how it is currently managed.

Tel (709) 729-6309/1-877-729-6309
Email: commissioner@oipc.nl.ca
www.oipc.nl.ca