Innovation, Science and Economic Development Canada

Office of the Corporate Secretary – ATIP Services Branch

PRIVACY MANAGEMENT FRAMEWORK

Rev. March 2025

Table of Contents

INTRODUCTION

Preamble

The *Privacy Act* (the Act) guarantees individuals the right of access to and correction of their personal information which may be held by Government of Canada (GoC) institutions, and regulates the collection, use and disclosure of personal information contained therein.

Treasury Board of Canada Secretariat (TBS) policies, including the Policy on Privacy Protection, the Directive on Personal Information Requests and Correction of Personal Information, and the Directive on Privacy Impact Assessment, further guide GoC institutions in their ongoing stewardship of privacy, and of personal information, in a multitude of areas, including:

- privacy breach management;
- privacy and consent statements;
- incidental collections of personal information;
- facilitating individuals' access to their personal information;
- Personal Information Banks; and
- training requirements for Public Servants.

Among GoC institutions, the collection and use of personal information at Innovation, Science and Economic Development Canada (ISED) is relatively minor. ISED is nevertheless, fully committed to ensuring compliance with privacy legislation and policies, including that the collection and use of personal information is authorized, necessary, specific, and transparent, and that its disclosure is consistent with legislative requirements.

This Privacy Management Framework is demonstrative of ISED's commitment to ensuring sound and compliant privacy practices.

Personal Information Definition

Personal Information is defined by paragraph 3 of the Act as, "Information about an identifiable individual that is recorded in any form." The specific type of information is practically limitless, but for the Public-at-large, includes (not an all-inclusive list): race; address; religious observance; age; marital status; education; criminal or employment history; finances; health information; a person's views or opinions about another individual; a

person's name where it appears with other personal information; blood type; fingerprints; interests; or an identifying number of symbol (such as a SIN, or employee number).

The Act deems that certain information that would ordinarily be deemed "personal" for the Public-at-large, are not personal in respect of Public Servants, and this information includes:

- that an individual is or was a government employee;
- the title, business address and contact information of a government employee;
- the classification, salary range and responsibilities held by a government employee;
- the name of a government employee appearing on documents prepared by the individual in the course of employment; and
- opinions or views expressed or given in the course of employment.

Departmental Privacy Lead
Within ISED, privacy administration falls under the responsibility of the ATIP Services Branch of the Office of the Corporate Secretary. The ATIP Services Branch can be contacted through one of the following channels:

- by email: ic.atip-aiprpa.ic@ised-isde.gc.ca;

- by telephone: 343-291-2788; or

- by postal mail: ISED ATIP Services Branch
  235 Queen St., 2nd Floor – West Tower
  OTTAWA ON K1A 0H5

MANAGING THE COLLECTION AND USE OF PERSONAL INFORMATION

Authority to Collect and Use Personal Information

The Act requires GoC institutions to possess legislative authority to collect and use personal information for their operating programs. The main authority that permits ISED to collect and use personal information is the

Department of Industry Act. Numerous other acts provide this authority to ISED, in relation to unique lines of business (i.e., telecommunications, intellectual property, bankruptcy, federally incorporated business entities, consumer affairs, etc.).

A complete list of acts that pertain to ISED's core mandate can be found at this hyperlink: List of acts.

Personal Information Banks

Personal information collected and used by ISED is described in Personal Information Banks (PIB) that detail the classes of individuals affected by the collections, in addition to other information about the purposes for which personal information is being collected, its permitted uses, and the correlating record numbers, and records retention and disposal information.

The ATIP Services Branch develops new PIBs to add to the departmental inventory, in cooperation with the relevant program officials, when new programs are implemented, and takes steps to withdrawal PIBs from the inventory when programs are wound-down. The Branch also cooperates closely with the TBS to effect PIB approvals and registrations.

Annotated Guide to Personal Information Banks and Classes of Personal Information

Incidental Collections of Personal Information

To reduce instances of incidental and over-collection of personal information, the ATIP Services Branch works with program officials to construct and add additional caveats to websites and feedback forms instructing individuals to not provide ISED with personal information, as required (such as when initiating Public Opinion Research or inviting public comments on proposed regulatory changes or program designs).

When information is incidentally collected within an information resource of business value (a record), the ATIP Services Branch advises program officials to annotate the personal information by identifying it as "personal" before saving it within regular program records. Identifying the information as "personal" helps to ensure that it is protected against disclosure if the

balance of the record is requested under an *Access to Information Act* process. When such incidental collections of personal information are transitory in nature, there is no requirement to retain it, and program officials are advised to destroy the information without saving it.

This protocol is supported by the fact that incidentally collected personal information is not pursuant to an approved PIB. As such, this category of information is neither required to be retained in a manner that facilitates the right of access pursuant to the Act, nor is it accessible through a request made under the Act.

Use of Personal Information for Non-Administrative Purposes
When personal information elements are to be used for non-administrative purposes at ISED—such as for statistical reporting, audit and evaluation, research and GBA+ activities—the information is depersonalized and aggregated prior to being used for those purposes.

When depersonalizing and aggregating personal information collected from small populations or sample sizes, further steps are taken to protect identity, which include:

- either not disclosing information from a small population that would permit reidentification of the individuals who provided personal information; or
- aggregating small population results, together with larger population results, to eliminate the possibility of reidentification.

Enhanced Policy on Using Personal Information for Non-Administrative Purposes

Privacy Requirements Incumbent on Contractors and Service Providers
When program delivery involving the collection or use of personal information is to be contracted to a service provider—such as under a single-recipient contribution program that further funds ultimate recipients, or the use of an identity validation service provider—the ATIP Services Branch works with the relevant program officials to ensure that requirements are built into contracts that compel service providers to

adequately protect privacy. Such requirements generally include (not an all-inclusive list):

- the requirement for the service provider to have its own privacy breach management protocol;
- restrictions that prohibit the service provider from using personal information for any purpose other than ISED's program delivery, including up-selling; and
- the requirement for the service provider to have a suitable records retention and disposal protocol that is compliant with all applicable legislation (such as [examples only] FINTRAC regulations, or the *PIPEDA*).

FACILITATING PERSONAL INFORMATION REQUESTS

Info Source

Info Source documents ISED's entire catalogue of operating programs and services, consistent with its annual Departmental Framework for Results. This document is published on ISED's public-facing Transparency website (see: ATIP Disclosures), and cross-referenced on its public-facing ATIP Services website. The publication further details:

- the types of information holdings in relation to each operating activity, including personal information;
- PIBs that support the collection and use of personal information;
- classes of personal records; and
- manuals in use by all operating programs.

Access to Personal Information (Privacy Requests)

ISED employs an efficient ATIP Services program, of some 30 employees, that facilitates the right of access by individuals to their personal information under the control of the department, as provided by the Act.

Due to the nature of ISED's core mandate, the department typically receives fewer than 40 such requests annually. Nevertheless, robust processing procedures—deferential to Access to Information procedures—

are in use, to ensure that program officials exercise the utmost confidentiality in treating these requests. For example:

- steps are taken to ensure that the identity of a requestor is disclosed to program officials only when absolutely necessary in order to facilitate the retrieval of information;
- when it is necessary to disclose the identity of a requestor, it is sent to the relevant program officials in an encrypted communication that is separate to the original case assignment; and
- when returning responsive information to the ATIP Services Branch, department officials use alternate means of transmission, to ensure that personal information is not uploaded to general repositories where greater numbers of employees would be able to access it.

The ATIP Services Branch is further supported by a Policy Division, that develops and delivers privacy training, responds to questions on privacy legislation and operational policy, and monitors compliance with all TBS policies and directives pertaining to Privacy, including the Policy on Privacy Protection and the Directive on Personal Information Requests and Correction of Personal Information. Such policy supports help to further facilitate privacy protection, as well as the right of access to personal information and the right to correction and annotation.

Personal Information Requests to Support Criminal Investigations
ISED receives numerous requests annually from investigative bodies recognized by the *Privacy Regulations*, and other law enforcement agencies, to support criminal investigations.

All such requests are managed solely by the ATIP Services Branch Policy Division, which ensures that the requesting parties have the right of access under the Act, and works with the relevant program officials across ISED to facilitate the retrievals and disclosures of the pertinent information.

Requests to Change or Annotate Personal Information
ISED logs all requests to change or annotate personal information in a case management system, and provides a full step-by-step protocol for changing and annotating information, on its ATIP Services Website, where it may be

accessed by all ISED employees at: Correcting and Annotating Personal Information.

ISED administers numerous programs and services that require personal information to be held in the public domain, by law. Such programs cover federally incorporated business entities, intellectual property, bankruptcy and insolvency, and others. When a program's founding legislation requires personal information to be held in the public domain, requests to correct or annotate personal information held by those programs are generally refused, pursuant to the applicable legislative requirements. For example:

- requests to delete or change information held in the public record about Directors of federally incorporated companies;
- requests to delete public information about bankrupt or insolvent individuals held in the public record; and
- requests to remove personal information about a copyright or trademark owner from the Intellectual Property Database.

PRIVACY PROTECTION THROUGH POLICY EXPERTISE

Privacy Impact Assessments

Privacy Impact Assessments (PIA) are the component of privacy management that focuses on the risks to individuals associated with the collection and use of their personal information, and what strategies should be implemented to mitigate those risks. A PIA serves as a "privacy playbook" or "roadmap" in relation to an operating program that collects and uses personal information, and fully documents the following components:

- Relevant program officials;
- Legislative authority that permits the collection of personal information;
- Description of the program or activity that uses personal information;
- Personal Information Banks associated with the collection;
- Shared responsibilities (such as, with other institutions);
- Analysis of personal information elements to be collected;

- Risk identification and categorization;
- Risk mitigation strategies;
- Information flows and access points;
- Technology concerns; and
- Demonstrative compliance with requirements

The ATIP Services Branch works directly with program officials to develop PIAs. The Branch provides a robust Annotated Guide to Privacy Impact Assessments and Privacy Protocols—including evergreen requirements—and the relevant PIA templates on its intranet site, at:

- Annotated Guide to Privacy Impact Assessments and Privacy Protocols

Consistent with requirements, completed PIAs are shared with the TBS and the Office of the Privacy Commissioner. Ensuing advice from those institutions is considered and, where applicable, incorporated into subsequent PIA updates.

Pursuant to the TBS Directive on Privacy Impact Assessment, an institution's delegate for section 10 of the *Privacy Act* may deem that a full, core PIA is not required in respect of a program or operating activity (such as when the collection and use of personal information is either minimal or negligible). When the ISED delegate for section 10 of the *Privacy Act* (the Director, ATIP Services) deems that a full, core PIA is not warranted, the ATIP Services Branch works with the relevant program officials to document a fulsome privacy analysis, in lieu of a PIA.

Privacy Notice Statements (Privacy Notices)
Pursuant to the TBS Directive on Privacy Practices, individuals must be adequately notified of the following key elements, when their personal information is to be collected:

- The legislative authority that permits the collection;
- The purpose of the collection, including all consistent uses;
- The PIB associated with the collection;

- The legal or administrative consequences for refusing to provide personal information;
- The right to have personal information corrected or annotated; and
- The right to complain to the Privacy Commissioner of Canada regarding an institution's handling of personal information.

The ATIP Services Branch works with program officials to develop TBS-compliant Privacy Notices for all operating programs and activities that collect and use personal information.

Though consent is not required to use personal information where legislation permits it to be collected and used, the ATIP Services Branch encourages departmental officials to incorporate consent capture mechanisms into Privacy Notices whenever possible, in an effort to ensure that individuals whose personal information is being collected and used are as informed as possible, and works with program officers to construct these mechanisms.

For those circumstances where personal information will be disclosed to a third party for a use that is consistent with the purpose of collection, the ATIP Services Branch requires a consent capture mechanism to appear together, with the balance of the Privacy Statement, to ensure that individuals' consent is well informed.

Consultations with the Office of the Privacy Commissioner
Consistent with requirements, ISED consults with officials from the Office of the Privacy Commissioner to obtain views and advice, prior to making new collections of personal information, and considers that input in its development of subsequent PIAs and PIBs.

Privacy Breach Management Tools
Breaches of personal information have the potential to cause harm for individuals that ranges from negligible, to extremely grave, depending on the nature and level of information breached. It is therefore important, when privacy breaches occur, that they be contained immediately, that the concerned individuals be notified, if appropriate, and that strategies are implemented to mitigate further occurrences of similar breaches.

To that effect, the ATIP Services Branch has developed a multi-faceted Privacy Breach Tool Kit that focuses on containment, assessment, mitigation and reporting.

The Privacy Breach Tool Kit is available to all employees, on the ATIP Services internal website at: Privacy Breach Management Tools.

PRIVACY PROTECTION THROUGH PROACTIVE DISCLOSURE REVIEWS

Proactive Publication Pre-Reviews

The ATIP Services Branch facilitates numerous proactive disclosures annually, the majority of which are made pursuant to the *Access to Information Act*. All such information is reviewed by ATIP Practitioners in advance of disclosure to ensure that personal information is not inadvertently disclosed in content such as:

- Question Period notes and cards;
- Transition briefing materials for newly appointed ministers and deputy heads;
- Materials used by ministers and deputy heads for their appearances before Committees of Parliament; and
- Reports on audits and evaluations of ISED programs and services.

Parliamentary Disclosure Pre-Reviews

ISED receives an average of 220 Enquiries of Ministry (order paper questions) annually, from both the House of Commons and the Senate. The proposed responses are reviewed by ATIP Practitioners in advance of disclosure, to ensure that personal information is not disclosed therein.

PRIVACY TRAINING AND AWARENESS

Training Programs

Enhanced awareness and knowledge of Privacy obligations on the part of departmental officials has shown to improve the quality of responses and ISED's rate of compliance with legislative and policy requirements in this

regard. To that end, the ATIP Services Branch offers the following facilitated training programs to all employees, on an on-demand basis:

- ATIP 101 at ISED: An overview of the legislation, associated timelines, and processes, as well as the role of the Department, the courts, and the Information and Privacy Commissioners of Canada, combined with a more in-depth look at the exempting and excluding provisions of the Access to Information Act, focusing on the top three such provisions used most frequently at ISED. This session is also offered in a modified format, when requested, to focus solely on either the Access to Information Act or the Privacy Act.

- Enhanced Training for ATIP Practitioners: A more in-depth look at some training elements required by the TBS Policy on Personal Information Requests and Correction of Personal Information for Public Servants who have delegated or functional ATIP responsibilities. Privacy related information includes: extensions of time limits; language, format and method of access requirements; public reporting requirements and the roles of Parliamentary Committees and the Privacy Commissioner;

- Personal Information Boot Camp for ISED: Comprehensive training focused solely on the Privacy Act and its related policy requirements, including the concept of 'informed consent,' privacy notice statements, privacy impact assessments, and privacy breach administration. This includes an in-depth look at the type and volume of personal information that exists at ISED, and the requirements surrounding the collection and use of personal information in relation to ISED and other Government of Canada programs.

ATIP Services Website:

The ATIP Services Branch maintains an internal website where all ISED employees can access and download various policies, guidance, coaching, training, checklists, procedures, legislation, news, and other ATIP-related information, including:

- Privacy Impact Assessment Policy and User Guide (and template);
- Privacy Breach Management Tool Kit;
- Privacy training (various offerings);
- Information on privacy in the context of audio-visual recordings in which Public Servants appear (and guidance on recording Public Servants doing their jobs);
- Correcting and annotating personal information;
- Advice on non-disclosure agreements; and
- Best practices for using MS Teams.