# CHAPTER 4

# ADMINISTRATION

## DIVISION 1 – ACCESS AND PRIVACY OFFICERS AND ACCESS TO INFORMATION REGISTRY

Section 84 – Access and privacy officer

Section 85 – Access to information registry

Section 86 – Compliance protocols

## DIVISION 2 – PUBLIC BODIES

Section 87 – Designated officer for public body

Section 88 – Additional duties and powers of head of public body

# Chapter 4 Overview

The ATIPP Office is Government of Yukon's central office for the *Access to Information and Protection of Privacy Act* (ATIPP Act). The ATIPP Office is the point of contact between the public and public bodies subject to the Act.

Employees of the ATIPP Office have been delegated duties and functions from the Access and Privacy Officer (APO) under the ATIPP Act.

Despite these delegations, the APO may still perform any of the powers, duties or functions if required.

The **ATIPP Act Coordinator** provides the day-to-day support to the Access and Privacy Officer by responding to ATIPP questions and is responsible for:

- Acting as the point of contact of the ATIPP Office;
- Receiving access requests;
- Working with the applicant and public body to formulate requests;
- Activating requests;
- Notifying the APO of a potential refusal of an access request;
- Receiving Access to Information Summaries from public bodies;
- Receiving notifications from Designated Access Officers and Heads of public bodies as required under the Act on behalf of the APO;
- Forwarding public body's final responses to applicants; and
- Maintaining the Access to Information Registry.

The **Manager Access & Privacy** is responsible for supporting the day-to-day functions of the ATIPP Act Coordinator by:

- Determining cost estimates;
- Notifying the applicant and public body of a cost estimate;
- Abandonment of access request; and
- Working with the applicant and public body to formulate requests.

The manager is responsible for the ATIPP Office's Central Shared Services analyst pool.

**ATIPP Office Central Shared Services** is a pool of Access and Privacy Analysts. The analyst positions are designated as the Designated Access Officers (DAOs) for select ministerial public bodies through a service level agreement and by designation of the head of each ministerial body. These analysts perform the duties and functions of the Designated Access Officer under the Act. They provide assistance with privacy breach assessments for the same ministerial public bodies they support under access.

The **Senior Access and Privacy Analyst** is responsible for

- general privacy questions;
- assisting public bodies' compliance with the ATIPP Act by creating and implementing protocols, policies, guidance, manuals, toolkits, templates and training;
- assistance with privacy impact assessments (PIAs) including providing reviews and recommendations;
- assisting Designated Privacy Officers with assessing and responding to privacy breaches;
- Receiving breach reports for breaches that involve risk of significant harm to individuals when the breach occurs within a Ministerial public body; and
- Conducting compliance inspections and providing inspection reports and recommendations to public bodies.

The Senior Access and Privacy Analyst is supported by a Privacy Compliance Specialist.

# PART 4

D1

## DIVISION 1 – ACCESS AND PRIVACY OFFICER AND ACCESS TO INFORMATION REGISTRY

### SECTION 84 Access and Privacy Officer

This provision establishes the statutory officer role of the Access and Privacy Officer (APO) with its authority and responsibilities under the ATIPP Act. This provision authorizes the minister responsible for this Act (Minister of the Department of Highways and Public Works) to appoint an employee of a public body to be the Access and Privacy Officer.

**"ACCESS AND PRIVACY OFFICER"** means the employee of a public body appointed as the access and privacy officer under subsection 84(1).

The Access and Privacy Officer replaces the previous *ATIPP* Act position of Records Manager. The Director of Corporate Information Management, appointed as the Access and Privacy Officer, oversees the ATIPP Office.

> **84(1)** The minister responsible for this Act must appoint an employee of a public body as the access and privacy officer.
>
> **84(2)** The access and privacy officer must
>
> **84(2)(a)** if they consider it necessary to do so in order to promote compliance with this Act, conduct an inspection of a public body, or a program or activity of a public body, to assess its compliance with this Act;

**Subsection 84(2)(a)** states the Access and Privacy Officer may conduct compliance inspections/audits of public bodies to ensure compliance with this Act. This responsibility is intended to allow government to proactively assess / measure compliance.

For example, the Access and Privacy Officer can inspect how a privacy breach has been assessed and reported to ensure public bodies are identifying breaches that involve risk of significant harm to individuals, as well as ensuring the proper processes being followed including notifications to individuals, heads, and the Information and Privacy Commissioner, as required by the act.

> **84(2)(b)** exercise or perform any prescribed power or duty; and

This provision gives cabinet the ability to prescribe additional functions the Access and Privacy Officer must fulfill.

> **84(2)(c)** delegate, in writing, any of their duties or powers under this Act (except the power to delegate under this paragraph) to another employee of a public body, subject to any conditions on the exercise of the delegated power or the performance of the delegated duty that the access and privacy officer considers appropriate.

**Subsection (2)(c)** allows the Access and Privacy Officer to delegate any of their responsibilities, except the ability to delegate. This enables the functional operations of the ATIPP Office.

> **84(3)** As soon as practicable after the completion of an inspection under paragraph (2)(a), the access and privacy officer must provide to the head of the public body to which the inspection relates an inspection report setting out their findings from the inspection and their recommendations, if any, to improve the compliance of the public body, or a program or activity of the public body, with this Act.

This provision requires the Access and Privacy Officer to create an inspection report and provide it to the head, including any recommendations to improve compliance.

## SECTION 85 Access to Information Registry

The registry consists of information about privacy impact assessments, summary of responses to access requests, compliance materials such as protocols that public bodies must adhere to, and additional information that aids in the compliance of the ATIPP Act.

Under **Section 85**, it is necessary that the Access and Privacy Officer creates an "access to information registry". The purpose of this registry is to have information about access and privacy easily accessible to the public.

**"ACCESS TO INFORMATION REGISTRY"** means the registry established under subsection 85(1).

> **85(1)** The access to information registry is established.
>
> **85(2)** The access and privacy officer
>
> **85(2)(a)** subject to subsection (3), may deposit into the access to information registry the following information or records:
>
> **85(2)(a)(i)** information about each privacy impact assessment conducted by the head of a public body,

This provision requires the access and privacy officer to post a summary of each Privacy Impact Assessment (PIA) received. For more on PIAs, please see Chapter 2.

**Subsection 85(2)(a)(ii)** requires the Access and Privacy Officer to make the summary of the ATIPP request response or the summary the head provides publicly available.

> **85(2)(a)(ii)** each response by a head under section 64 (or if it is impracticable to do so, a summary of the response) together with a summary of the access request for which the response was provided,

**Subsection 85(2)(a)(iii)** requires the Access and Privacy Officer to make binding protocols available to the public. These protocols will assist public bodies with compliance with the Act.

> **85(2)(a)(iii)** a protocol, the rules of which are to be binding on public bodies or, if specified in the protocol, a class of public bodies,

**Subsection 85(2)(a)(iv)** gives the Access and Privacy Officer discretion to deposit any other information into the registry required to improve compliance with the Act, for example, creating service standards for public bodies to implement and then report publicly on the results.

> **85(2)(a)(iv)** any other information that the access and privacy officer considers would, if made known to public bodies by depositing it into the registry, promote and strengthen public bodies' compliance with this Act; and

**Subsection 85(2)(b)** places an obligation on the Access and Privacy Officer to ensure information in the registry is up-to-date and complete. The importance of accuracy and completeness in the registry is emphasized in this provision.

> **85(2)(b)** must maintain the information and records deposited into the access to information registry in an accurate and complete form.

**Subsection 3** requires the Access and Privacy Officer to review the exceptions to access that a head may use to deny information and remove any information that must not be disclosed, for example, confidential third party business information.

> **85(3)** Before depositing a record into the access to information registry, the access and privacy officer must remove from the record all information to which access is prohibited under Division 8 of Part 3 or to which the head of a responsive public body may deny access under Division 9 of Part 3.

In order for public bodies to comply with this section of the Act, the head must establish a review process within the ministerial public body to ensure that any mandatory or discretionary exceptions to access are applied to the material. Heads may choose to delegate this responsibility to their Designated Access Officer (DAO) or Designated Privacy Officer (DPO).

## SECTION 86 Compliance Protocols

This provision gives the Access and Privacy Officer (APO) the authority to create binding protocols for public bodies.

These protocols are intended to improve compliance with the Act by establishing common standards for public bodies to follow, for example, requiring ministerial bodies to use specific forms such as a privacy impact assessment template and a privacy breach reporting form.

> **86(1)** For the purpose of the consistent administration of, and compliance by public bodies with, this Act, the access and privacy officer may establish rules in a protocol
>
> **86(1)(a)** respecting the scope or description of a program or activity of a public body or a service provided by the program or activity;

This provision allows the Access and Privacy Officer to clarify the scope of critical terms in the act: program, activity and service. Understanding and applying these terms properly are key in evaluating compliance in how personal information is being collected, used and disclosed.

> **86(1)(b)** specifying the forms, and any additional procedures, to be used for
>
> **86(1)(b)(i)** conducting a privacy impact assessment,

This provision allows Access and Privacy Officer to specify the forms and procedures required for public bodies to follow when undertaking a PIA.

For example, the Access and Privacy Officer can require ministerial bodies to complete PIAs using a specific form and require ministerial bodies to submit the PIA to the Access and Privacy Officer for review.

> **86(1)(b)(ii)** providing a notice to an individual under paragraph 32(7)(b) or 83(2)(a), or

This provision allows the Access and Privacy Officer to establish specific forms/procedures to notify affected individuals in the event of a privacy breach or health or safety issue.

> **86(1)(b)(iii)** preparing an access information summary;

This provision allows the Access and Privacy Officer to establish additional rules for preparing an access to information summary.

**"ACCESS INFORMATION SUMMARY"**, in respect of an access request, means the written summary provided to the Access and Privacy Officer under section 53 for the access request.

An access information summary includes the necessary information for the Access and Privacy Officer to determine a cost estimate.

**Subsection 86(1)(c)** allows the Access and Privacy Officer to clarify when a PIA is required under provision 11(1)(e) – when a significant change is made to the collection, use or disclosure of personal information. An example, changes that will be requiring PIAs for any new system a program or activity may deploy.

> **86(1)(c)** for determining whether a privacy impact assessment must be conducted under paragraph 11(1)(e), including
>
> **86(1)(c)(i)** specifying criteria for determining whether a change is a significant change, or
>
> **86(1)(c)(ii)** specifying a type of action considered to be a significant change;

**Subsection 86(1)(d)** allows for the Access and Privacy Officer to establish standards for Designated Privacy Officers to assist in evaluating whether an unauthorized collection or privacy breach occurred.

> **86(1)(d)** specifying criteria to be considered by a designated privacy officer when assessing a report under subsection 14(1) or 32(2);

**Subsection 86(1)(e)** allows the Access and Privacy Officer to create government standards for making personal information publicly available, including information found in a registry.

> **86(1)(e)** respecting the manner in which a public body makes the following personal information available to the public:
>
> **86(1)(e)(i)** publicly available information,

**86(1)(e)(ii)** information contained in a public registry;

**Subsection 86(1)(f)** allows the Access and Privacy Officer to establish government standards for specific types of agreements identified in the act: specialized services (see **section 27**), information management service (see **section 28**), data-linking (see **section 29**) and research agreements (see **section 26**). These standards will identify the specific terms and conditions that must be included in agreements.

**86(1)(f)** specifying additional terms and conditions that must be included in an agreement referred to in subsection 26(1), paragraphs 27(e), 28(1)(e) and 29(e), and subsection 33(3);

**Subsection 86(1)(g)** allows the access and privacy officer to establish standards when creating an open access register.

**"OPEN ACCESS REGISTER"**, of a public body means the open access register established under paragraph 41(1)(a). See Chapter 3, Division 2 for more on Open Access.

**86(1)(g)** specifying methods for establishing an open access register;

**86(1)(h)** allows for different types of public bodies to be treated differently, taking into consideration the ministerial public bodies that have different applicable provisions under the Act.

**86(1)(i)** applying different rules of a protocol to different groups, types or classes of public bodies; or

**86(1)(j)** respecting any other matter that the access and privacy officer considers necessary to promote and strengthen public bodies' administration of and compliance with this Act.

**Subsection (1)(j)** gives the Access and Privacy Officer the flexibility to create protocols on other issues that promote compliance with the Act.

**Subsection 2** states that a protocol is binding on all public bodies, or all public bodies of a class of public bodies when it is deposited in the Access to Information Registry.

**86(2)** Each rule contained in a protocol is binding on all public bodies, or all public bodies of a class of public bodies as specified in the protocol, beginning on the day on which the access and privacy officer deposits the protocol into the access to information registry and ending on the day on which the access and privacy officer removes the protocol from the registry.

**Subsection 3** clarifies that a protocol is not a regulation. A regulation provides detail on how to apply the Act and requires Cabinet approval. A protocol is a set of binding rules to ensure consistency and compliance with the Act.

> **86(3)** A protocol and each rule contained in it are not regulations within the meaning of the *Regulations Act*.

**Subsection 4** requires the Access and Privacy Officer to provide a proposed protocol to the Information and Privacy Commissioner (IPC) for comment 15 business days before being deposited in the access to information registry. This provides the IPC with the ability to make comments to strengthen the protocols compliance measures.

> **86(4)** Not later than 15 business days before the access and privacy officer deposits a protocol into the access to information registry, they must provide a copy of it to the commissioner for review and recommendations, if any.

**Subsection 5** clarifies that non-binding guidelines can be written by the Access and Privacy Officer.

**86(5)** For greater certainty, nothing in this section limits the access and privacy officer's ability to establish non-binding guidelines respecting administrative matters under this Act.

# PART 4

## DIVISION 2 – PUBLIC BODIES

### SECTION 87 Designated officer for public body

This provision requires a head to appoint a Designated Privacy Officer (DPO) and Designated Access Officer (DAO).

**"HEAD"**, of a public body, means a ministerial body (Government of Yukon department of corporation); or a statutory body or entity (non-statutory body) prescribed through ATIPP Regulations. Please see the ATIPP Regulations for a full breakdown of who is considered a public body, statutory body or non-statutory body (entity). Public bodies include **"EMPLOYEES"** and **"SERVICE PROVIDERS"**.

**"DESIGNATED ACCESS OFFICER"**, of a public body, means an employee designated under paragraph 87(1)(b) as a designated access officer for the public body.

**"DESIGNATED PRIVACY OFFICER"**, of a public body, means the employee designated under paragraph 87(1)(a) as a designated access officer for the public body.

> **87(1)** The head of a public body must designate in writing
>
> **87(1)(a)** an employee of a public body as the designated privacy officer for the public body; and
>
> **87(1)(b)** at least one employee of a public body as a designated access officer for the public body.

**Subsection 87(1)(a)** requires that there be one specific employee designated as the Designated Privacy Officer (DPO) for a public body. The purpose for only designating one DPO is to maintain accountability of the public body on privacy matters.

**Subsection (1)(b)** requires that a Designated Access Officer (DAO) be appointed for a public body. There may be more than one DAO appointed for a public body, or one DAO may be appointed in respect of multiple public bodies. This approach enables the government to provide a centralization of processing access requests.

**Subsection 87(2**) clarifies that a head may choose to have the same individual as the privacy officer and access officer – the *Designated Access and Privacy Officer (DAPO)*.

> **87(2)** For greater certainty

**87(2)(a)** an employee of a public body may be designated as both the designated privacy officer and a designated access officer for a public body;

**87(2)(b)** the head of a public body may designate one or more employees as designated access officers for the public body; and

**Subsections 7(2)(b) and (2)(c)** clarify that one or more individuals can be designated as the access officer. This is to enable a centralized pool of analysts to process ATIPP requests, through an integrated service agreement. For more on integrated services, see **section 27** of this Chapter.

## SECTION 88 Additional duties and powers of head of public body

This provision that clarifies how the head must respond to an audit conducted by either the Access and Privacy Officer (APO) or Information and Privacy Commissioner (IPC). The IPC may only conduct audits on privacy matters related to personal information. This provision also enables the head to delegate any of their duties or powers under the act to an employee of a public body.

The **"HEAD"** of a public body, is responsible for all decisions made under the *ATIPP Act* that relate to that public body. If the public body is a department, branch or office in Government of Yukon, the head is the member of the Executive Council (the Minister) who presides over the public body (**section 1**)**.**

**"MINISTER RESPONSIBLE"**, for a department, means the Minister appointed under the *Government Organisation Act* to preside over the department.

**"DEPARTMENT"** has the same meaning as in the *Government Organisation Act*. "DEPARTMENT ", means a department in the public service and includes an agency, branch, commission, board, or corporation of the Government of Yukon.

For other public bodies that are not ministerial public bodies (i.e. Statutory and Non-Statutory bodies or entities), the head is the person designated as the head through *ATIPP Act Regulations*.

> **88** The head of a public body
>
> **88(a)** must, if requested to do so by the access and privacy officer in respect of an inspection of the public body under paragraph 84(2)(a), ensure that the public body provides to the access and privacy officer
>
> **88(a)(i)** the information and records requested that are relevant to the matter being inspected, and
>
> **88(a)(ii)** reasonable assistance during the inspection;
>
> **88(b)** must, as requested by the commissioner in respect of the conduct of a privacy compliance audit of the public body under paragraph 111(1)(b), ensure that the public body provides to the commissioner
>
> **88(b)(i)** the information and records requested that are relevant to the matter being audited, and
>
> **88(b)(ii)** reasonable assistance during the audit; and

> **88(c)** may delegate, in writing, any of their duties or powers under this Act (except the power to delegate under this paragraph) to an employee of a public body, subject to any conditions on the exercise of the delegated power or the performance of the delegated duty that the head considers necessary.

Under **section 84(2)(c)** of the Act, the head of a public body has the power to delegate to a employee of a public body any of the head's duties, powers and functions under the Act, except the power to delegate.

In a small public body, where the designated head may also be the *Designated Access and Privacy Officer (DAPO)*, there will generally be no need to delegate. In larger public bodies, a delegation document may be needed.

All public bodies that decide to delegate some or all of the head's powers and duties should have a current delegation document in place. It should be reviewed with a new head to confirm that the head agrees with the scheme of delegated responsibilities.

The delegation document should identify the position, not the individual, to which the powers are delegated. When delegation is to the position rather than the person, a new delegation is not required when a new appointee assumes the position or when someone is acting in the position. A delegation document may also recognize another position to which delegation passes if the occupant of the original position is absent.

A delegation document may cover a wide variety of duties, powers and functions, under the ATIPP Act. A delegation document remains in effect until it is replaced. It is important to review the document periodically for any changes that may be needed, especially if the public body is restructured or part of the public body is transferred to another public body.

There is a substantial difference between delegations relating to Part 3, Access to Information, and those relating to Part 2, Protection of Privacy. In the case of access to information, the delegations relate mostly to the processing of an access request and the decision whether or not to disclose all or part of a record. In the case of privacy protection, responsibilities centre on the collection, handling and protection of personal information. This is a much more general area of responsibility and is centred on the program areas or local offices that handle the information on a day-today basis. Even in small public bodies, most privacy protection responsibilities should be delegated to staff in the program areas responsible for the information.

Not every section of the Act dealing with privacy matters calls for delegation of responsibility in a formal sense. The head of a public body should, however, clearly advise program administrators and managers of their responsibilities, especially with regard to compliance in the collection and disclosure of personal information.

It is essential when a delegation document is put in place that all identified officers or employees know and understand their delegated responsibilities. It is also important for other officers and employees to understand that only those with delegated responsibilities under the ATIPP Act should be carrying out those duties or functions.

All hiring documents or materials for employees should include a statement about ATIPP Act responsibilities for each official or employee taking up a position that includes delegated responsibilities under the Act. The employee should also be advised that additional information can be obtained from the ATIPP Office.

If the individual with delegated authority does not actually make the decision that he or she has been authorized to make, the delegation has not been properly exercised. Once a delegate makes a valid determination or decision in the proper exercise of the delegated power, the head of the public body cannot re-determine the matter or substitute his or her decision for that of the delegate.

For more on heads responsibilities and designating officers under the Act, see the ATIPP Office's Toolkit for Heads of Public Bodies.