Privacy – Know The Laws Of Your Province

Privacy protection regulations are vital for ensuring the secure handling of personal information within public and private institutions. These regulations require organizations to collect personal data only for authorized and necessary purposes, maintain its accuracy, and protect it against unauthorized access, use, or disclosure. Key measures include mandatory breach reporting, secure data storage, access and correction rights for individuals, and privacy impact assessments for new programs. While the principles of privacy protection are consistent across Canada, each province and territory establishes specific requirements tailored to its legal and operational context. Compliance with these regulations safeguards individual rights, prevents misuse of information, and strengthens public trust in institutional practices.

FEDERAL

Under the Privacy Act **Sections Section 4, 5(1), 6(1), 7, 8(1)(2), 12(1), 13 to 15**, **employers** in government institutions **must** collect personal information only when necessary, directly from the individual when possible, and retain it for reasonable access. They **must** ensure the information is used and disclosed only for authorized purposes and protect it from misuse. **Employers** are also responsible for responding to access requests and ensuring compliance with privacy rights, helping maintain trust and legal accountability in the workplace.

Collection, Retention, and Disposal of Personal Information

Collection of Personal Information

No personal information **shall** be collected by a government institution unless it relates directly to an operating program or activity of the institution. **Section 4.**

Personal Information to be Collected Directly

(1) A government institution **shall**, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates except where the individual authorizes otherwise or where personal information may be disclosed to the institution under subsection 8(2). **Section 5.**

Retention of Personal Information used for an Administrative Purpose

(1) Personal information that has been used by a government institution for an administrative purpose **shall** be retained by the institution for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information. **Section 6.**

Protection of Personal Information

Use of Personal Information

Personal information under the control of a government institution **shall** not, without the consent of the individual to whom it relates, be used by the institution except:

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or

(b) for a purpose for which the information may be disclosed to the institution under subsection 8(2). **Section 7.**

Disclosure of Personal Information

(1) Personal information under the control of a government institution **shall** not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

Where Personal Information may be Disclosed

(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed:

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;

(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;

(d) to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;

(e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;

(f) for the purpose of administering or enforcing any law or carrying out a lawful investigation, under an agreement or arrangement between the Government of Canada or any of its institutions and any of the following entities or any of their institutions:

(i) the government of a foreign state,

(ii) an international organization of states or an international organization

established by the governments of states,

(iii) the government of a province,

(iv) the council of the Westbank First Nation,

(v) the council of a participating First Nation as defined in subsection 2(1) of the First Nations Jurisdiction over Education in British Columbia Act,

(vi) the council of a participating First Nation as defined in section 2 of the Anishinabek Nation Education Agreement Act,

(vii) a First Nation Government or the Anishinabek Nation Government, as defined in section 2 of the Anishinabek Nation Governance Agreement Act, or an Anishinaabe Institution, within the meaning of section 1.1 of the Agreement, as defined in section 2 of that Act,

(vii.1) the Whitecap Dakota Government, as defined in section 2 of the Self-Government Treaty Recognizing the Whitecap Dakota Nation / Wapaha Ska Dakota Oyate Act;

(g) to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem;

(h) to officers or employees of the institution for internal audit purposes, or to the office of the Comptroller General or any other person or body specified in the regulations for audit purposes;

(i) to the Library and Archives of Canada for archival purposes;

(j) to any person or body for research or statistical purposes if the head of the government institution:

(i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and

(ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates;

(k) to any aboriginal government, association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada;

(l) to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and

(m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.
Section 8 (1)(2).

For more information:

- Access to Personal Information – Right of Access. **Sections 12.**
- Requests for Access. **Sections 13.**
- Notice where access requested. **Sections 14.**
- Extension of time limits. **Sections 15.**

Further details on the Privacy Act can be found at justice.gc.ca.

ALBERTA

Under the Alberta **Human Rights Act Section 3 and Section 10**, and the **Personal Information Protection Act Sections 7(1), 8(1), 11, 13, 24, 25 and 34**, **employers must** ensure the privacy and dignity of individuals by avoiding discriminatory publications and protecting personal information. **Employers** are responsible for obtaining consent before collecting, using, or disclosing personal data, limiting collection to what is reasonable, notifying individuals of data use, providing access to and correction of records, and implementing security measures to prevent unauthorized access or misuse.

Alberta Human Rights Act

Code of Conduct

Discrimination re: Publications, Notices

(1) No person **shall** publish, issue or display or cause to be published, issued or displayed before the public any statement, publication, notice, sign, symbol, emblem, or other representation that:

(a) indicates discrimination or an intention to discriminate against a person or a class of persons, or

(b) is likely to expose a person or a class of persons to hatred or contempt because of the race, religious beliefs, colour, gender, gender identity, gender expression, physical disability, mental disability, age, ancestry, place of origin, marital status, source of income, family status, or sexual orientation of that person or class of persons.

(2) Nothing in this section **shall** be deemed to interfere with the free expression of opinion on any subject.

(3) Subsection (1) does not apply to:

(a) the display of a notice, sign, symbol, emblem, or other representation displayed to identify facilities customarily used by one gender,

(b) the display or publication by or on behalf of an organization that:

(i) is composed exclusively or primarily of persons having the same political or religious beliefs, ancestry or place of origin, and

(ii) is not operated for private profit, of a statement, publication, notice, sign, symbol, emblem, or other representation indicating a purpose or membership qualification of the organization, or

(c) the display or publication of a form of application or an advertisement that may be used, circulated or published pursuant to section 8(2), if the statement,

publication, notice, sign, symbol, emblem, or other representation is not derogatory, offensive, or otherwise improper. **Section 3.**

Prohibitions Regarding Complaints

(1) No person **shall** retaliate against a person because that person:

(a) has made or attempted to make a complaint under this Act,

(b) has given evidence or otherwise participated in or may give evidence or otherwise participate in a proceeding under this Act,

(c) has made or is about to make a disclosure that person may be **required** to make in a proceeding under this Act, or

(d) has assisted in any way in:

(i) making or attempting to make a complaint under this Act, or

(ii) the investigation, settlement, or prosecution of a complaint under this Act.

(2) No person **shall**, with malicious intent, make a complaint under this Act that is frivolous or vexatious. **Section 10.**

Personal Information Protection Act

Division 2 — Consent

Consent Required

(1) Except where this Act provides otherwise, an organization **shall** not, with respect to personal information about an individual,

(a) collect that information unless the individual consents to the collection of that information,

(b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source,

(c) use that information unless the individual consents to the use of that information, or

(d) disclose that information unless the individual consents to the disclosure of that information. **Section 7.**

Form of Consent

(1) An individual may give his or her consent in writing or orally to the collection, use or disclosure of personal information about the individual. **Section 8.**

Division 3 — Collection of Personal Information

Limitations on Collection

(1) An organization may collect personal information only for purposes that are reasonable.

(2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is

collected. **Section 11.**

Notification Required for Collection

(1) Before or at the time of collecting personal information about an individual from the individual, an organization **must** notify that individual in writing or orally:

(a) as to the purposes for which the information is collected, and

(b) of the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.

(2) Repealed 2009 c50 s6.

(3) Before or at the time personal information about an individual is collected from another organization without the consent of the individual, the organization collecting the personal information **must** provide the organization that is disclosing the personal information with sufficient information regarding the purpose for which the personal information is being collected in order to allow the organization that is disclosing the personal information to make a determination as to whether that disclosure of the personal information would be in accordance with this Act.

(4) Subsection (1) does not apply to the collection of personal information that is carried out pursuant to section 8(2). **Section 13.**

For more information:

- Division 1 – Access and Correction – Access to records and provision of information. **Sections 24 (1) to (4).**
- Right to request correction. **Sections 25 (1) to (5).**
- Protection of information. **Sections 34.**

Further details on the Occupational Health and Safety Code can be found at alberta.ca.

BRITISH COLUMBIA

Under the **Human Rights Code Section 7, 22** and the **Personal Information Protection Act Sections 6(1), 7(1), 11, 13, 16, 23 and 24**, **employers** in British Columbia **must** ensure that workplace practices respect both non-discrimination in communications and the protection of personal information. **Employers** are prohibited from publishing materials that indicate or incite discrimination, and they **must** obtain valid consent before collecting, using, or disclosing personal data. They are also responsible for limiting collection to reasonable purposes, notifying employees of data use, ensuring secure handling of personal information, and responding to access or correction requests.

Human Rights Code

Discriminatory Publication

(1) A person **must** not publish, issue or display, or cause to be published, issued or displayed, any statement, publication, notice, sign, symbol, emblem or other representation that:

(a) indicates discrimination or an intention to discriminate against a person or a group or class of persons, or

(b) is likely to expose a person or a group or class of persons to hatred or contempt because of the Indigenous identity, race, colour, ancestry, place of origin, religion, marital status, family status, physical or mental disability, sex, sexual orientation, gender identity or expression, or age of that person or that group or class of persons.

(2) Subsection (1) does not apply to a private communication, a communication intended to be private or a communication related to an activity otherwise permitted by this Code. **Section 7 (1)(2).**

Time Limit for Filing a Complaint

(1) A complaint **must** be filed within one year of the alleged contravention.

(2) If a continuing contravention is alleged in a complaint, the complaint **must** be filed within one year of the last alleged instance of the contravention.

(3) If a complaint is filed after the expiration of the time limit referred to in subsection (1) or (2), a member or panel may accept all or part of the complaint if the member or panel determines that:

(a) it is in the public interest to accept the complaint, and

(b) no substantial prejudice will result to any person because of the delay. **Section 22.**

Personal Information Protection Act

Part 3 – Consent

Consent Required

(1) An organization **must** not:

(a) collect personal information about an individual,

(b) use personal information about an individual, or

(c) disclose personal information about an individual. **Section 6.**

Provision of Consent

(1) An individual has not given consent under this Act to an organization unless:

(a) the organization has provided the individual with the information **required** under section 10 (1), and

(b) the individual’s consent is provided in accordance with this Act.

(2) An organization **must** not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service.

(3) If an organization attempts to obtain consent for collecting, using or disclosing personal information by:

(a) providing false or misleading information respecting the collection, use or disclosure of the information, or

(b) using deceptive or misleading practices any consent provided in those circumstances is not validly given. **Section 7 (1) to (3).**

For more information:

- Part 4 – Collection of Personal Information – Limitations on collection of personal information. **Sections 11.**
- Collection of employee personal information. **Section 13.**
- Use of employee personal information. **Section 16.**
- Right to request correction of personal information. **Section 24.**

Further details on the Human Rights Code and Personal Information Protection Act can be found at gov.bc.ca.

MANITOBA

Under **The Human Rights Code Section 9(1)(a) and 39(3)** and **The Personal Health Information Act Sections 13(1), 20(1), 22(1), 23, 6 and 11**, Manitoba **employers** and health trustees **must** protect personal health information by collecting, using, and disclosing it only for lawful and necessary purposes. Individuals have the right to access and correct their information, and disclosures—such as to family or for fundraising—are allowed only under strict conditions.

The Human Rights Code

PART II – PROHIBITED CONDUCT AND SPECIAL PROGRAMS

"Discrimination" Defined

(1) In this Code, **"discrimination"** means:

(a) differential treatment of an individual on the basis of the individual's actual or presumed membership in or association with some class or group of persons, rather than on the basis of personal merit; **Section 9.**

Public Hearing

(3) Every hearing **shall** be open to the public, but in order to prevent undue prejudice to any party or witness, the adjudicator may prohibit publication or broadcasting of the identity of the party or witness until the adjudicator's final decision has been rendered. **Section 39.**

The Personal Health Information Act

PART 2 – ACCESS TO PERSONAL HEALTH INFORMATION

RIGHT TO EXAMINE AND COPY PERSONAL HEALTH INFORMATION

Trustee to Respond Promptly

(1) A trustee **shall** respond to a request as promptly as **required** in the circumstances but not later than:

(a) 24 hours after receiving it, if the trustee is a hospital and the information is about health care currently being provided to an in-patient;

(b) 72 hours after receiving it, if the information is about health care the trustee

is currently providing to a person who is not a hospital in-patient; and

(c) 30 days after receiving it in any other case, unless the request is transferred to another trustee under section 8.

Information Provided in 24 Hours

(1.1) In the circumstance mentioned in clause (1)(a) (hospital patient), the trustee is **required** only to make the information available for examination and need not, despite section 7, provide a copy.

Duty to Assist an Individual

(2) A trustee **shall** make every reasonable effort to assist an individual making a request and to respond without delay, openly, accurately and completely.

Failure to Respond

(3) The failure of a trustee to respond to a request within the time frame **required** under subsection (1) is to be treated as a decision to refuse to permit the personal health information to be examined or copied. **Section 6 (1) to (3).**

REASONS FOR REFUSING ACCESS

Reasons for Refusing Access

(1) A trustee is not **required** to permit an individual to examine or copy his or her personal health information under this Part if:

(a) knowledge of the information could reasonably be expected to endanger the health or safety of the individual or another person;

(b) disclosure of the information would reveal personal health information about another person who has not consented to the disclosure;

(c) disclosure of the information could reasonably be expected to identify a third party, other than another trustee, who supplied the information in confidence under circumstances in which confidentiality was reasonably expected;

(d) the information was compiled and is used solely:

(i) for the purpose of peer review by health professionals,

(ii) for the purpose of review by a standards committee established to study or evaluate health care practice in a health care facility or health services agency,

(iii) for the purpose of a body with statutory responsibility for the discipline of health professionals or for the quality or standards of professional services provided by health professionals, or

(iv) for the purpose of risk management assessment; or

(e) the information was compiled principally in anticipation of, or for use in, a civil, criminal, or quasi-judicial proceeding. **Section 11 (1).**

For more information:

- DIVISION 1 — RESTRICTIONS ON COLLECTION AND RETENTION OF INFORMATION. **Sections 13(1).**

- GENERAL DUTIES OF TRUSTEES. **Section 20(1).**
- Restrictions on use of information. **Section 21(1).**
- Timely disclosure to family. **Section 23(1.1).**
- Disclosure about patient's condition. **Section 23(2).**
- No disclosure if possible harm. **Section 23(3).**
- Disclosure to religious organization. **Section 23.1(1).**
- **Section 23.2(1).**
- Disclosure for fundraising. **Section 23.2(2).**

Further details on the Human Rights Code and the Personal Health Information Act can be found at gov.mb.ca.

NEW BRUNSWICK

In New Brunswick, **employers** and public bodies are responsible for protecting personal data under the **Right to Information and Protection of Privacy Act, Sections 37 to 40, 43 to 46**, and the **Personal Health Information Privacy and Access Act, Sections 3(1), 20, 22**. These laws require that personal information only be collected if authorized and necessary, that it be accurate, and that it be used or disclosed solely for permitted purposes. **Employers must** ensure individuals are informed about data collection and are given access and correction rights.

Right to Information and Protection of Privacy Act

PROTECTION OF PRIVACY

Collection, Correction, and Retention of Personal Information

Collection of Personal Information

(1) Personal information may be collected by or for a public body only if the collection of the information is authorized or **required** by or under an Act of the Legislature or an Act of the Parliament of Canada.

(2) Despite subsection (1), personal information may also be collected by or for a public body without the collection of the information being authorized or **required** by or under an Act of the Legislature or an Act of the Parliament of Canada if:

(a) the information relates directly to and is necessary for:

(i) a service, program, or activity of the public body, or

(ii) a common or integrated service, program, or activity,

(b) the information is collected for law enforcement purposes, or

(c) the information is collected by or for the public body for the purpose for which the information was disclosed to it under a provision of section 46 or 46.1.

(3) A public body **shall** collect only as much personal information about an individual as is reasonably necessary to accomplish the purpose for which it is collected. **Section 37 (1) to (3).**

Restrictions on Use and Disclosure of Personal Information

General Duty of Public Bodies

(1) A public body **shall** not use or disclose personal information except as authorized under this Division.

(2) Every use and disclosure by a public body of personal information **must** be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed.

(3) A public body **shall** limit the use and disclosure of personal information in its custody or under its control to those of its officers, directors, employees or agents who need to know the information to carry out the purpose for which the information was collected or received or to carry out a purpose authorized under section 44. **Section 43 (1) to (3).**

Use of Personal Information

A public body may use personal information only:

(a) for the purpose for which the information was collected or compiled under subsection 37(1) or (2) or for a use consistent with that purpose,

(a.1) for the purpose for which the information was collected or compiled under section 37.1 or for a use consistent with that purpose,

(b) if the individual the information is about has consented to the use,

(c) for a purpose for which that information may be disclosed by the public body under section 46, 46.1, 47 or 48 or for a use approved under section 47,

(d) for the purpose for which that information was disclosed to the public body under section 46, 46.1, 47 or 48, or

(e) for the purpose of producing de-identified information that does not, either by itself or in combination with other information in the custody or under the control of the public body, permit an individual to be identified. **Section 44.**

Personal Health Information Privacy and Access Act

Application

(1) This Act applies:

(a) to personal health information that is collected, used or disclosed by a custodian or an agent or that is in the custody or control of a custodian or an agent, and

(b) to personal health information that was collected before the coming into force of this Act and that is prescribed by regulation. **Section 3.**

Refusal to Consent or Withdrawal of Consent

(1) An individual may refuse to grant his or her consent or withdraw his or her consent to the collection, use or disclosure of the individual’s personal health information by a custodian except if:

(a) it is prohibited by law to withdraw consent,

(b) the collection, use, or disclosure is for the purposes of a program to monitor the prescribing, dispensing or use of certain classes of drugs,

(c) the collection, use or disclosure is for the purposes of the creation or maintenance of an electronic health record, or

(d) the collection, use or disclosure is for another purpose provided for in this Act.

(2) If an individual refuses to grant consent or withdraws his or her consent to the collection, use or disclosure of his or her personal health information under subsection (1), the custodian **shall:**

(a) take reasonable steps to act in accordance with the decision,

(b) inform the individual of the implications of the refusal or withdrawal, and

(c) inform the other custodians, if any, holding the individual's personal health information of the decision.

(3) A custodian may refuse to comply with the refusal or withdrawal of an individual's consent to the collection, use or disclosure of his or her personal health information under subsection (1) if compliance with the individual's refusal or withdrawal of consent is likely to endanger the health of the individual or the health of another person.

(4) If the custodian refuses to comply with the refusal or withdrawal of an individual's consent for the reasons referred to in subsection (3), the custodian **shall** inform the individual, as soon as possible, of the collection, use or disclosure of his or her personal health information. **Section 22 (1) to (4).**

For more information:

- Collection of personal information. **Sections 37 (1)(2).**
- Manner of collection. **Sections 38 (1).**
- Right to request correction of personal information. **Sections 40 (1) to (7).**
- Disclosure of personal information. **Sections 46 (1) to (7).**
- Mandatory disclosure of personal information for common or integrated services, programs or activities. **Sections 46.1 to 46.3.**
- Personal Health Information Privacy and Access Act. **Section 3.**
- Conditional consent. **Section 20.**
- Assumption of validity. **Section 21.**

Further details on the Right to Information and Protection of Privacy Act and Personal Health Information Privacy and Access Act can be found at laws.gnb.ca and laws.gnb.ca.

NEWFOUNDLAND & LABRADOR

In Newfoundland and Labrador, **employers** and public bodies **must** comply with the **Access to Information and Protection of Privacy Act, Sections 61–68 and 73**, which strictly govern the collection, use, and disclosure of personal information. **Employers** are responsible for ensuring that information is collected lawfully, accurately maintained, and only used or disclosed for legitimate and limited purposes. Reasonable safeguards **must** be in place to protect personal data from unauthorized access or breaches, and any incident posing significant harm **must** be reported.

Protection of Personal Information

(1) The head of a public body **shall** take steps that are reasonable in the circumstances to ensure that:

(a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;

(b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and

(c) records containing personal information in its custody or control are retained, transferred, and disposed of in a secure manner.

(2) For the purpose of paragraph (1)(c), “disposed of in a secure manner” in relation to the disposition of a record of personal information does not include the destruction of a record unless the record is destroyed in such a manner that the reconstruction of the record is not reasonably foreseeable in the circumstances.

(3) Except as otherwise provided in subsections (6) and (7), the head of a public body that has custody or control of personal information **shall** notify the individual who is the subject of the information at the first reasonable opportunity where the information is:

(a) stolen;

(b) lost;

(c) disposed of, except as permitted by law; or

(d) disclosed to or accessed by an unauthorized person.

(4) Where the head of a public body reasonably believes that there has been a breach involving the unauthorized collection, use or disclosure of personal information, the head **shall** inform the commissioner of the breach.

(5) Notwithstanding a circumstance where, under subsection (7), notification of an individual by the head of a public body is not **required**, the commissioner may recommend that the head of the public body, at the first reasonable opportunity, notify the individual who is the subject of the information.

(6) Where a public body has received personal information from another public body for the purpose of research, the researcher may not notify an individual who is the subject of the information that the information has been stolen, lost, disposed of in an unauthorized manner or disclosed to or accessed by an unauthorized person unless the public body that provided the information to the researcher first obtains that individual’s consent to contact by the researcher and informs the researcher that the individual has given consent.

(7) Subsection (3) does not apply where the head of the public body reasonably believes that the theft, loss, unauthorized disposition, or improper disclosure or access of personal information does not create a risk of significant harm to the individual who is the subject of the information.

(8) For the purpose of this section, “significant harm” includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

(9) The factors that are relevant to determining under subsection (7) whether a

breach creates a risk of significant harm to an individual include:

(a) the sensitivity of the personal information; and

(b) the probability that the personal information has been, is being, or will be misused. **Section 64 (1) to (9).**

Retention of Personal Information

(1) Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body **shall** retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

(2) A public body that has custody or control of personal information that is the subject of a request for access to a record or correction of personal information under Part II **shall** retain that information for as long as necessary to allow the individual to exhaust any recourse under this Act that he or she may have with respect to the request. **Section 65(1)(2).**

Use of Personal Information

(1) A public body may use personal information only:

(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose as described in section 69 ;

(b) where the individual the information is about has identified the information and has consented to the use, in the manner set by the minister responsible for this Act; or

(c) for a purpose for which that information may be disclosed to that public body under sections 68 to 71.

(2) The use of personal information by a public body **shall** be limited to the minimum amount of information necessary to accomplish the purpose for which it is used. **Section 66 (1)(2).**

For more information:

- Use of personal information by post-secondary educational bodies. **Sections 67 (1) to (4).**
- Disclosure of personal information. **Sections 68 (1)(8).**
- DIVISION 2 — PRIVACY COMPLAINT. **Sections 73 (1) to (5).**

Further details on the Access to Information and Protection of Privacy Act can be found at assembly.nl.ca.

NOVA SCOTIA

In Nova Scotia, **employers** and public bodies **must** manage personal data responsibly under the **Freedom of Information and Protection of Privacy Act, Sections 24, 26, and 27. Employers** are **required** to collect only the personal information necessary for lawful and essential operations, ensure its accuracy if used to make decisions about individuals, and protect it with reasonable security measures. Use and disclosure of personal information are strictly limited to authorized purposes, with written consent, or as **required** by law. **Employers must** also retain such information for at

least one year to allow individuals reasonable access, reinforcing accountability and safeguarding privacy in the workplace.

PROTECTION OF PERSONAL PRIVACY: COLLECTION, PROTECTION, RETENTION,

USE, AND DISCLOSURE OF PERSONAL INFORMATION

Treatment of Personal Information

(1) Personal information **shall** not be collected by or for a public body unless:

(a) the collection of that information is expressly authorized by or pursuant to an enactment;

(b) that information is collected for the purpose of law enforcement; or

(c) that information relates directly to and is necessary for an operating program or activity of the public body.

(2) Where an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body **shall** make every reasonable effort to ensure that the information is accurate and complete.

(3) The head of the public body **shall** protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

(4) Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body **shall** retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it. **Section 24 (1) to (4).**

Use of Personal Information

A public body may use personal information only:

(a) for the purpose for which that information was obtained or compiled, or for a use compatible with that purpose;

(b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use; or

(c) for a purpose for which that information may be disclosed to that public body pursuant to Sections 27 to 30. **Section 26 (a) to (c).**

Disclosure of Personal Information

A public body may disclose personal information only:

(a) in accordance with this Act or as provided pursuant to any other enactment;

(b) if the individual the information is about has identified the information and consented in writing to its disclosure;

(c) for the purpose for which it was obtained or compiled, or a use compatible with that purpose;

(d) for the purpose of complying with an enactment or with a treaty, arrangement or agreement made pursuant to an enactment;

(e) for the purpose of complying with a subpoena, warrant, sum- mons or order issued or made by a court, person or body with jurisdiction to compel the production of information;

(f) to an officer or employee of a public body or to a minister, if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister;

(g) to a public body to meet the necessary requirements of gov- ernment operation;

(h) for the purpose of:

(i) collecting a debt or fine owing by an individual to His Majesty in right of the Province or to a public body, or

(ii) making a payment owing by His Majesty in right of the Province or by a public body to an individual;

(i) to the Auditor General or any other prescribed person or body for audit purposes;

(j) to a member of the House of Assembly who has been requested by the individual, whom the information is about, to assist in resolving a problem;

(k) to a representative of the bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry;

(l) to the Public Archives of Nova Scotia, or the archives of a public body, for archival purposes;

(m) to a public body or a law-enforcement agency in Canada to assist in an investigation:

(i) undertaken with a view to a law-enforcement proceeding, or

(ii) from which a law-enforcement proceeding is likely to result;

(n) if the public body is a law-enforcement agency and the information is disclosed:

(i) to another law-enforcement agency in Canada, or

(ii) to a law-enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority;

(o) if the head of the public body determines that compelling circumstances exist that affect anyone’s health or safety;

(p) so that the next of kin or a friend of an injured, ill or deceased individual may be contacted; or

(q) in accordance with Section 29 or 30. **Section 27 (a) to (q).**

Further details on the Freedom of Information and Protection of Privacy Act can be found at canlii.org.

NORTHWEST TERRITORIES

In the Northwest Territories, **employers** and public bodies are **required** to protect

personal data under the Access to Information and **Protection of Privacy Act**, **specifically Sections 40, 41, 42, 43, 44, and 48**. **Employers must** collect personal information only when legally authorized, for law enforcement, or when necessary for approved programs. They are also responsible for informing individuals of the purpose and legal basis for collection, ensuring accuracy if the information is used to make decisions, and protecting it against unauthorized use or disclosure. Use and disclosure are limited to original or consistent purposes, with consent, or as legally **required**.

PART 2 – PROTECTION OF PRIVACY

DIVISION A – COLLECTION OF PERSONAL INFORMATION

Purpose of Collection of Information

No personal information may be collected by or for a public body unless:

(a) the collection of the information is expressly authorized by an enactment;

(b) the information is collected for the purposes of law enforcement; or

(c) the information relates directly to and is necessary for:

(i) an existing program or activity of the public body, or

(ii) a proposed program or activity where collection of the information has been authorized by the head with the approval of the Executive Council. **Section 40 (a) to (c).**

Collection of Information from Individual Concerned

(1) A public body **must**, where reasonably possible, collect personal information directly from the individual the information relates to unless:

(a) another method of collection is authorized by that individual or by an enactment;

(b) the information may be disclosed to the public body under Division C of this Part;

(c) the information is collected for the purpose of law enforcement;

(d) the information is collected for the purpose of collecting a fine or a debt owed to the Government of the Northwest Territories or a public body;

(e) the information concerns the history, release or supervision of an individual under the control or supervision of a correctional authority;

(f) the information is collected for the purpose of providing legal services to the Government of the Northwest Territories or a public body;

(g) the information:

(i) is necessary in order to determine the eligibility of an individual to participate in a program of or receive a benefit, product or service from the Government of the Northwest Territories or a public body and is collected in the course of processing an application made by or on behalf of the individual the information is about, or

(ii) is necessary in order to verify the eligibility of an individual who is

participating in a program of or receiving a benefit, product or service from the Government of the Northwest Territories or a public body and is collected for that purpose;

(g.1) subject to the regulations, the information is disclosed to a public body, where the information is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee to whom the information is disclosed;

(h) the information is collected for the purpose of informing the Public Trustee about potential clients;

(i) the information is collected for the purpose of enforcing a maintenance order under the Maintenance Orders Enforcement Act; or

(j) the information is collected for the purpose of hiring, managing or administering personnel of the Government of the Northwest Territories or a public body.

Notice to Individual

(2) A public body that collects personal information directly from the individual the information is about **shall** inform the individual of:

(a) the purpose for which the information is collected,

(b) the specific legal authority for the collection, and

(c) the title, business address and business telephone number of an officer or employee of the public body who can answer questions about the collection, unless the regulations provide that this subsection does not apply to that type of information.

Exceptions

(3) Subsections (1) and (2) do not apply if:

(a) the collection is for law enforcement purposes; or

(b) the head of the public body concerned determines that compliance with those subsections might:

(i) result in the collection of inaccurate information, or

(ii) defeat the purpose or prejudice the use for which the information is collected. **Section 41. (1) to (3).**

Protection of Personal Information

The head of a public body **shall** protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. **Section 42.**

Definition: “Privacy Impact Assessment”

(1) In this section, “privacy impact assessment” means an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or service, including a common or integrated program or service, meets or will meet the requirements of this Part.

Privacy Impact Assessment

(2) Subject to subsection (3), a public body **shall**, during the development of a proposed enactment, system, project, program or service that involves the collection, use or disclosure of personal information, prepare and submit a privacy impact assessment to the head of the public body for review and comment.

Common or Integrated Program or Service

(3) The head of a public body, with respect to a common or integrated program or service, **shall**, during the development of the proposed program or service, prepare and submit a privacy impact assessment to the Information and Privacy Commissioner for review and comment.

Notification of a Common or Integrated Program or Service

(4) The head of a public body **must** notify the Information and Privacy Commissioner of a common or integrated program or service at an early stage of developing the program or service. **Section 42.1. (1) to (4).**

For more information:

- DIVISION B — USE OF PERSONAL INFORMATION. **Sections 43 to 46.**
- DIVISION C — DISCLOSURE OF PERSONAL INFORMATION. **Sections 47, 48.**

Further details on the Access to Information and Protection of Privacy Act can be found at gov.nt.ca.

NUNAVUT

In Nunavut, **employers** and public bodies are **required** to protect personal data under the Access to Information and **Protection of Privacy Act, specifically Sections 40, 41, 42, 43, 44, and 48**. **Employers must** collect personal information only when legally authorized, for law enforcement, or when necessary for approved programs. They are also responsible for informing individuals of the purpose and legal basis for collection, ensuring accuracy if the information is used to make decisions, and protecting it against unauthorized use or disclosure. Use and disclosure are limited to original or consistent purposes, with consent, or as legally **required**.

PART 2 — PROTECTION OF PRIVACY

DIVISION A — COLLECTION OF PERSONAL INFORMATION

Purpose of Collection of Information

No personal information may be collected by or for a public body unless:

(a) the collection of the information is expressly authorized by an enactment;

(b) the information is collected for the purposes of law enforcement; or

(c) the information relates directly to and is necessary for:

(i) an existing program or activity of the public body, or

(ii) a proposed program or activity where collection of the information has been authorized by the head with the approval of the Executive Council. **Section 40 (a) to (c).**

Collection of Information from Individual Concerned

(1) A public body **must**, where reasonably possible, collect personal information directly from the individual the information relates to unless:

(a) another method of collection is authorized by that individual or by an enactment;

(b) the information may be disclosed to the public body under Division C of this Part;

(c) the information is collected for the purpose of law enforcement;

(d) the information is collected for the purpose of collecting a fine or a debt owed to the Government of the Northwest Territories or a public body;

(e) the information concerns the history, release or supervision of an individual under the control or supervision of a correctional authority;

(f) the information is collected for the purpose of providing legal services to the Government of the Northwest Territories or a public body;

(g) the information:

(i) is necessary in order to determine the eligibility of an individual to participate in a program of or receive a benefit, product or service from the Government of the Northwest Territories or a public body and is collected in the course of processing an application made by or on behalf of the individual the information is about, or

(ii) is necessary in order to verify the eligibility of an individual who is participating in a program of or receiving a benefit, product or service from the Government of the Northwest Territories or a public body and is collected for that purpose;

(g.1) subject to the regulations, the information is disclosed to a public body, where the information is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee to whom the information is disclosed;

(h) the information is collected for the purpose of informing the Public Trustee about potential clients;

(i) the information is collected for the purpose of enforcing a maintenance order under the Maintenance Orders Enforcement Act; or

(j) the information is collected for the purpose of hiring, managing or administering personnel of the Government of the Northwest Territories or a public body.

Notice to Individual

(2) A public body that collects personal information directly from the individual the information is about **shall** inform the individual of:

(a) the purpose for which the information is collected,

(b) the specific legal authority for the collection, and

(c) the title, business address and business telephone number of an officer or employee of the public body who can answer questions about the collection, unless the

regulations provide that this subsection does not apply to that type of information.

Exceptions

(3) Subsections (1) and (2) do not apply if:

(a) the collection is for law enforcement purposes; or

(b) the head of the public body concerned determines that compliance with those subsections might:

(i) result in the collection of inaccurate information, or

(ii) defeat the purpose or prejudice the use for which the information is collected. **Section 41. (1) to (3).**

Protection of Personal Information

The head of a public body **shall** protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. **Section 42.**

Definition: "Privacy Impact Assessment"

(1) In this section, "privacy impact assessment" means an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or service, including a common or integrated program or service, meets or will meet the requirements of this Part.

Privacy Impact Assessment

(2) Subject to subsection (3), a public body **shall**, during the development of a proposed enactment, system, project, program or service that involves the collection, use or disclosure of personal information, prepare and submit a privacy impact assessment to the head of the public body for review and comment.

Common or Integrated Program or Service

(3) The head of a public body, with respect to a common or integrated program or service, **shall**, during the development of the proposed program or service, prepare and submit a privacy impact assessment to the Information and Privacy Commissioner for review and comment.

Notification of a Common or Integrated Program or Service

(4) The head of a public body **must** notify the Information and Privacy Commissioner of a common or integrated program or service at an early stage of developing the program or service. **Section 42.1. (1) to (4).**

For more information:

- DIVISION B – USE OF PERSONAL INFORMATION. **Sections 43 to 46.**
- DIVISION C – DISCLOSURE OF PERSONAL INFORMATION. **Sections 47, 48.**

Further details on the Access to Information and Protection of Privacy Act can be found at gov.nt.ca.

ONTARIO

In Ontario, under the Freedom of Information and **Protection of Privacy Act**, **Sections 38 to 42**, **employers must** ensure personal information is collected lawfully, used only for authorized or consistent purposes, and protected against unauthorized access or disclosure. Data used in decisions **must** be accurate, securely retained, and disposed of properly. Breaches that pose a real risk of significant harm **must** be reported to both the individual and the Commissioner.

PART III – PROTECTION OF INDIVIDUAL PRIVACY

Collection and Retention of Personal Information

Personal Information

(1) In this section and in section 39, "personal information" includes information that is not recorded and that is otherwise defined as "personal information" under this Act.

Collection of Personal Information

(2) No person **shall** collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity. **Section 38 (1)(2).**

Manner of Collection

(1) Personal information **shall** only be collected by an institution directly from the individual to whom the information relates unless,

(a) the individual authorizes another manner of collection;

(b) the personal information may be disclosed to the institution concerned under section 42 or under section 32 of the *Municipal Freedom of Information and Protection of Privacy Act*;

(c) the Commissioner has authorized the manner of collection under clause 59 (c);

(d) the information is in a report from a reporting agency in accordance with the *Consumer Reporting Act*;

(e) the information is collected for the purpose of determining suitability for an honour or award to recognize outstanding achievement or distinguished service;

(f) the information is collected for the purpose of the conduct of a proceeding or a possible proceeding before a court or tribunal;

(g) the information is collected for the purpose of law enforcement; or

(h) another manner of collection is authorized by or under a statute.

Notice to Individual

(2) Where personal information is collected on behalf of an institution, the head **shall**, unless notice is waived by the responsible minister, inform the individual to whom the information relates of,

(a) the legal authority for the collection;

(b) the principal purpose or purposes for which the personal information is intended to be used; and

(c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

Exception

(3) Subsection (2) does not apply where the head may refuse to disclose the personal information under subsection 14 (1) or (2) (law enforcement), section 14.1 (*Civil Remedies Act, 2001*) or section 14.2 (*Prohibiting Profiting from Recounting Crimes Act, 2002*). **Section 39 (1) to (3).**

Retention and Protection of Personal Information

(1) Personal information that has been used by an institution **shall** be retained after use by the institution for the period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to personal information.

Standard of Accuracy

(2) The head of an institution **shall** take reasonable steps to ensure that personal information on the records of the institution is not used unless it is accurate and up to date.

Exception

(3) Subsection (2) does not apply to personal information collected for law enforcement purposes.

Disposal of Personal Information

(4) A head **shall** dispose of personal information under the control of the institution in accordance with the regulations. **Section 40 (1) to (4).**

Use of Personal Information

(1) An institution **shall** not use personal information in its custody or under its control except,

(a) where the person to whom the information relates has identified that information in particular and consented to its use;

(b) for the purpose for which it was obtained or compiled or for a consistent purpose;

(c) for a purpose for which the information may be disclosed to the institution under section 42 or under section 32 of the *Municipal Freedom of Information and Protection of Privacy Act*; or

(d) subject to subsection (2), an educational institution may use personal information in its alumni records and a hospital may use personal information in its records for the purpose of its own fundraising activities, if the personal information is reasonably necessary for the fundraising activities. **Section 41 (1).**

For more information:

- Privacy impact assessment. **Section 38 (3)(4)(5).**
- Breach of privacy safeguards. **Section 40.1 (1) to (11).**
- Notice on using personal information for fundraising. **Section 41 (2).**
- Discontinuing use of personal information. **Section 41 (3).**
- Where disclosure permitted. **Section 42 (1).**
- Notice on disclosing personal information for fundraising. **Section 42 (2).**
- Fundraising agreement. **Section 42 (3).**

Further details on the Freedom of Information and Protection of Privacy Act can be found at ontario.ca.

PRINCE EDWARD ISLAND

In Prince Edward Island, under the **Freedom of Information and Protection of Privacy Act, Sections 31 to 33 and 36 to 37**, **employers** and public bodies **must** collect, use, and disclose personal information only for authorized purposes, such as law enforcement or program delivery. Information **must** be collected directly from the individual when possible, with proper notice. When personal information is used to make decisions about individuals, it **must** be accurate, retained for at least one year, and protected with reasonable security measures.

PART II – PROTECTION OF PRIVACY

Division 1 – Collection of Personal Information

Purpose of Collection of Information

No personal information may be collected by or for a public body unless:

(a) the collection of that information is expressly authorized by or under an enactment of Prince Edward Island or Canada;

(b) that information is collected for the purposes of law enforcement; or

(c) that information relates directly to and is necessary for an operating program or activity of the public body. **Section 31.**

Manner of Collection of Information

A public body **shall** collect personal information directly from the individual the information is about unless:

(a) another method of collection is authorized by:

(i) that individual,

(ii) another Act or a regulation under another Act, or

(iii) the Commissioner under clause 50(1)(f);

(b) the information may be disclosed to the public body under Division 2 of this Part;

(c) the information is collected for the purpose of law enforcement;

(d) the information is collected for the purpose of collecting a fine or a debt owed to the Government of Prince Edward Island or a public body;

(e) the information concerns the history, release or supervision of an individual under the control or supervision of a correctional authority;

(f) the information is collected for use in the provision of legal services to the Government of Prince Edward Island or a public body;

(g) the information is necessary:

(i) to determine the eligibility of an individual to participate in a program of or receive a benefit, product or service from the Government of Prince Edward Island or a public body and is collected in the course of processing an application made by or on behalf of the individual the information is about, or

(ii) to verify the eligibility of an individual who is participating in a program of or receiving a benefit, product or service from the Government of Prince Edward Island or a public body and is collected for that purpose;

(h) the information is collected for the purpose of informing the Public Trustee or a person exercising public guardianship functions about clients or potential clients;

(i) the information is collected for the purpose of enforcing a maintenance order under the Maintenance Enforcement Act R.S.P.E.I. 1988, Cap. M-1;

(j) the information is collected for the purpose of managing or administering personnel of the Government of Prince Edward Island or a public body;

(k) the information is collected for the purpose of assisting in researching or validating the claims, disputes or grievances of aboriginal people;

(l) the information is collected in a health or safety emergency where:

(i) the individual is not able to provide the information directly, or

(ii) direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or another person;

(m) the information concerns an individual who is designated as a person to be contacted in an emergency, or other specified circumstances;

(n) the information is collected for the purpose of determining suitability for an honour or award, including an honorary degree, scholarship, prize or bursary; or

(o) the information is collected from published or other public sources for the purpose of fundraising.

Right to be Informed

A public body that collects personal information that is **required** by subsection (1) to be collected directly from the individual the information is about **shall** inform the individual of:

(a) the purpose for which the information is collected;

(b) the specific legal authority for the collection; and

(c) the title, business address, and business telephone number of an officer or employee of the public body who can answer the individual’s questions about the collection.

Application of Subsections (1) and (2)

Subsections (1) and (2) do not apply if, in the opinion of the head of the public body concerned, compliance with them could reasonably be expected to result in the collection of inaccurate information. **Section 32.**

Accuracy of Personal Information

If an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body **shall:**

(a) make every reasonable effort to ensure that the information is accurate and complete; and

(b) retain the personal information for:

(i) the period **required** by the records retention and disposition schedule for the public body, as **required** by the Archives and Records Act or another enactment that applies with respect to that public body, or

(ii) if subclause (i) does not apply with respect to the public body, at least one year after using it. **Section 33.**

For more information:

- Division 2 — Use and Disclosure of Personal information by Public Bodies **Sections 36, 37.**

Further details on the Freedom of Information and Protection of Privacy Act can be found at princeedwardisland.ca.

QUÉBEC

In Quebec, **employers must** protect personal privacy as **required** under the **Charter of Human Rights and Freedoms, sections 5 and 9**, and the **Act Respecting the Protection of Personal Information in the Private Sector, sections 4 to 16 and 27**. Personal data can only be collected for serious, legitimate purposes and **must** be limited to what is necessary. It should be collected directly from the individual when possible, and individuals **must** be clearly informed of its use. **Employers must** ensure the data is accurate, secure, and only used or disclosed with valid consent or legal authorization.

Charter of Human Rights and Freedoms

PART I — HUMAN RIGHTS AND FREEDOMS

CHAPTER I — FUNDAMENTAL FREEDOMS AND RIGHTS

Every person has a right to respect for his private life. **Section 5.**

Every person has a right to non-disclosure of confidential information.

No person bound to professional secrecy by law and no priest or other minister of religion may, even in judicial proceedings, disclose confidential information revealed to him by reason of his position or profession, unless he is authorized to do so by the person who confided such information to him or by an express provision of law.

The tribunal **must** ensure that professional secrecy is respected. **Section 9.**

Act respecting the protection of personal information in the private sector

DIVISION II — COLLECTION OF PERSONAL INFORMATION

Any person carrying on an enterprise who, for a serious and legitimate reason, collects personal information on another person **must** determine the purposes for collecting the information before doing so. **Section 4.**

The personal information concerning a minor under 14 years of age may not be collected from him without the consent of the person having parental authority or of the tutor, unless collecting the information is clearly for the minor's benefit. **Section 4.1.**

Any person collecting personal information on another person may collect only the information necessary for the purposes determined before collecting it. **Section 5.**

Such information **must** be collected by lawful means.

Any person collecting personal information relating to another person may collect such information only from the person concerned, unless the latter consents to collection from third persons.

However, he may, without the consent of the person concerned, collect such information from a third person if the law so authorizes.

He may also do so if he has a serious and legitimate reason and either of the following conditions is fulfilled:

(1) the information is collected in the interest of the person concerned and cannot be collected from him in due time;

(2) collection from a third person is necessary to ensure the accuracy of the information. **Section 6.**

Any person collecting personal information from another person carrying on an enterprise **must**, at the request of the person concerned, inform the latter of the source of the information.

This section does not apply to a file established for the purposes of an inquiry to prevent, detect or repress a crime or statutory offence. **Section 7.**

Any person who collects personal information from the person concerned **must**, when the information is collected and subsequently on request, inform that person:

(1) of the purposes for which the information is collected;

(2) of the means by which the information is collected;

(3) of the rights of access and rectification provided by law; and

(4) of the person's right to withdraw consent to the communication or use of the information collected.

If applicable, the person concerned is informed of the name of the third person for whom the information is being collected, the name of the third persons or categories of third persons to whom it is necessary to communicate the information for the purposes referred to in subparagraph 1 of the first paragraph, and the possibility

that the information could be communicated outside Québec.

On request, the person concerned is also informed of the personal information collected from him, the categories of persons who have access to the information within the enterprise, the duration of the period of time the information will be kept, and the contact information of the person in charge of the protection of personal information.

The information **must** be provided to the person concerned in clear and simple language, regardless of the means used to collect the personal information. **Section 8 (1) to (4).**

In addition to the information that **must** be provided in accordance with section 8, any person who collects personal information from the person concerned using technology that includes functions allowing the person concerned to be identified, located or profiled **must** first inform the person:

(1) of the use of such technology; and

(2) of the means available to activate the functions that allow a person to be identified, located or profiled.

“Profiling” means the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person’s work performance, economic situation, health, personal preferences, interests or behaviour. **Section 8.1. (1)(2).**

Any person who collects personal information through technological means **must** publish on the enterprise’s website, if applicable, a confidentiality policy drafted in clear and simple language and disseminate it by any appropriate means to reach the persons concerned. The person **must** do the same for the notice **required** for any amendment to such a policy. **Section 8.2.**

Any person who provides his personal information in accordance with section 8 consents to its use and its communication for the purposes referred to in subparagraph 1 of the first paragraph of that section. **Section 8.3.**

No person may, after being notified by a credit assessment agent in accordance with section 9 of the Credit Assessment Agents Act (chapter A-8.2) of the existence of a security freeze prohibiting the agent from communicating personal information, request communication of that information from another credit assessment agent for the purposes of the same entering into a contract or the same credit increase for which a request had been made to the agent having sent the notice of the existence of the freeze. **Section 8.4.**

No person may refuse to respond to a request for goods or services or to a request relating to employment by reason of the applicant’s refusal to disclose personal information except where:

(1) collection of that information is necessary for the conclusion or performance of a contract;

(2) collection of that information is authorized by law; or

(3) there are reasonable grounds to believe that the request is not lawful.

In case of doubt, personal information is deemed to be non-necessary. **Section 9.**

Any person carrying on an enterprise who collects personal information when offering to the public a technological product or service having privacy settings **must** ensure that those settings provide the highest level of confidentiality by default, without any intervention by the person concerned.

The first paragraph does not apply to privacy settings for browser cookies. **Section 9.1.**

For more information:

- DIVISION III — CONFIDENTIALITY OF PERSONAL INFORMATION. **Sections 10 to 16.**
- DIVISION IV — ACCESS BY PERSONS CONCERNED. **Section 27.**

Further details on the Charter of Human Rights and Freedoms and Act Respecting the Protection of Personal Information in the Private Sector can be found at gouv.qc.ca and gouv.qc.ca.

SASKATCHEWAN

In Saskatchewan, **employers** and local authorities **must** protect privacy under **The Local Authority Freedom of Information and Protection of Privacy Act, sections 24 to 30**. Personal information can only be collected for purposes related to a local program or activity, preferably directly from the individual, and individuals **must** be informed of the collection purpose. Authorities **must** ensure accuracy, limit use to the original purpose or a consistent one, and restrict disclosure unless authorized by law or with consent. Individuals have the right to access their information, and any breach posing significant harm **must** be reported to the affected person.

PART IV — Protection of Privacy

Purpose of Information

No local authority **shall** collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the local authority. **Section 24.**

Manner of Collection

(1) A local authority **shall**, where reasonably practicable, collect personal information directly from the individual to whom it relates.

(2) A local authority that collects personal information that is **required** by subsection (1) to be collected directly from an individual **shall**, where reasonably practicable, inform the individual of the purpose for which the information is collected.

(3) Subsections (1) and (2) do not apply where compliance with them might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the information is collected. **Section 25.**

Standard of Accuracy

A local authority **shall** ensure that personal information being used by the local authority for an administrative purpose is as accurate and complete as is reasonably possible. **Section 26.**

Use of Personal Information

No local authority **shall** use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except:

(a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose; or

(b) for a purpose for which the information may be disclosed to the local authority pursuant to subsection 28(2). **Section 27.**

Notification

A local authority **shall** take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual. **Section 28. 28.1.**

Personal Information of Deceased Individual

(1) Subject to subsection (2) and to any other Act, the personal information of a deceased individual **shall** not be disclosed until 25 years after the death of the individual.

(2) Where, in the opinion of the head, disclosure of the personal information of a deceased individual to the individual's next of kin would not constitute an unreasonable invasion of privacy, the head may disclose that personal information before 25 years have elapsed after the individual's death. **Section 29(1)(2).**

Individual's Access to Personal Information

(1) Subject to Part III and subsections (2) and (3), an individual whose personal information is contained in a record in the possession or under the control of a local authority has a right to, and:

(a) on an application made in accordance with Part II; and

(b) on giving sufficient proof of his or her identity; **shall** be given access to the record.

(2) A head may refuse to disclose to an individual personal information that is evaluative or opinion material compiled solely for the purpose of determining the individual's suitability, eligibility or qualifications for employment or for the awarding of contracts and other benefits by the local authority, where the information is provided explicitly or implicitly in confidence.

(3) The head of the University of Saskatchewan or the University of Regina may refuse to disclose to an individual personal information that is evaluative or opinion material compiled solely for the purpose of:

(a) determining the individual's suitability for:

(i) appointment, promotion or tenure as a member of the faculty of the University of Saskatchewan or the University of Regina;

(ii) admission to an academic program; or

(iii) receipt of an honour or award; or

(b) evaluating the individual's research projects or materials for publication; where the information is provided explicitly or implicitly in confidence. **Section 30 (1) to (3).**

For more information:

- Disclosure of personal information. **Sections 28 (1)(2).**

Further details on the Local Authority Freedom of Information and Protection of Privacy Act can be found at canlii.org.

YUKON TERRITORY

In Yukon, under Access to Information and **Protection of Privacy Act, Sections 30 to 32, 34 to 36**, public bodies **must** protect personal information by securely managing it and responding swiftly to suspected breaches. Employees **must** report privacy breaches to designated privacy officers, who assess the risk of significant harm and notify affected individuals and the commissioner if necessary. Individuals have the right to access and request corrections to their personal information, and public bodies **must** respond within 30 business days.

PART 2 – PROTECTION OF PRIVACY

DIVISION 7 – PROTECTING PERSONAL INFORMATION

Securing Personal Information Against Privacy Breach

The head of a public body **must** protect personal information held by the public body by securely managing the personal information in accordance with the regulations. **Section 30.**

Employee to Report Suspected Privacy Breach

If an employee of a public body reasonably believes that a privacy breach in respect of personal information held by the public body has occurred or is occurring, the employee **must**, without delay, report the suspected privacy breach to the designated privacy officer for the public body. **Section 31.**

Response to Report of Suspected Privacy Breach

(1) In this section:

"affected individual", in respect of a privacy breach, means an individual whose personal information is personal information in respect of which a privacy breach has occurred or is occurring. « particulier touché »

(2) Without delay after receiving a report made under section 31, the designated privacy officer **must** assess the report.

(3) For the purpose of an assessment under subsection (2), the designated privacy officer for a public body may request from the head or an employee of the public body any information that the designated privacy officer considers necessary to conduct their assessment.

(4) Without delay after receiving a request under subsection (3), the head or employee who received the request **must**, if they hold the information requested, provide it to the designated privacy officer.

(5) If, after conducting their assessment under subsection (2), a designated privacy officer determines that a privacy breach has occurred or is occurring, the designated privacy officer **must**, without delay, determine, in accordance with subsection (6), whether there is a risk of significant harm to affected individuals due to the privacy breach.

(6) In making a determination under subsection (5), the designated privacy officer **must** consider the following factors in relation to the privacy breach to which the determination relates:

(a) the sensitivity of the personal information in respect of which the privacy breach has occurred or is occurring;

(b) the probability that the personal information is, has been or will be used or disclosed in an unauthorized manner;

(c) how much time elapsed between the occurrence of the privacy breach and the determination that it occurred;

(d) the number of affected individuals; d) le nombre de particuliers touchés;

(e) the type of relationship, if any, between affected individuals and any person who may have used, or to whom may have been disclosed, the personal information in respect of which the privacy breach has occurred or is occurring;

(f) the measures, if any, that the public body has implemented or is implementing to reduce the risk of significant harm to the affected individuals;

(g) if the personal information has been lost, stolen or disposed of, whether or not any of the personal information has been recovered;

(h) any other information that is relevant in the circumstances and is reasonably available to the designated privacy officer.

(7) If a designated privacy officer determines that there is a risk of significant harm to affected individuals due to a privacy breach, the designated privacy officer **must**, without delay after making the determination:

(a) notify the head of the public body of the privacy breach and the risk of significant harm to the affected individuals;

(b) provide to each affected individual, in accordance with the regulations and each applicable protocol, a notice of the privacy breach and the risk of significant harm to them;

(c) provide to the commissioner:

(i) a report made in accordance with subsection (8), and

(ii) a copy of the notice referred to in paragraph (b); and

(d) in the case of a privacy breach relating to a ministerial body, provide a copy of the report referred to in subparagraph (c)(i) to the access and privacy officer.

(8) A report made by a designated privacy officer under subparagraph (7)(c)(i) **must** include:

(a) the designated privacy officer’s reasons for determining that a risk of significant harm to the affected individuals exists;

(b) the designated privacy officer’s assessment of the cause of the privacy breach; and

(c) a description of each measure that the public body has implemented or is implementing to reduce the risk of significant harm to the affected individuals.

(9) On receiving a report made under subparagraph (7)(c)(i), the commissioner may recommend, in writing, to the head of the public body to which the report relates that the public body implement measures, as specified by the commissioner in the recommendation, that are likely to:

(a) reduce the risk of significant harm to the affected individuals; and

(b) prevent the occurrence of, or mitigate the effect of, a privacy breach in similar circumstances.

(10) Not later than 30 days after the day on which the head of a public body receives a recommendation under subsection (9), the head **must**, in respect of each measure specified in the recommendation:

(a) decide whether to require the public body to implement the measure; and

(b) provide a notice of their decision to the commissioner.

(11) If the head of a public body does not, within the applicable period, provide the notice referred to in paragraph (10)(b) in respect of a specific measure, the head is considered to have decided not to require the public body to implement the measure. **Section 32 (1) to (11).**

For more information:

- DIVISION 8 — ACCESSING AND CORRECTING PERSONAL INFORMATION. **Sections 34, 35.**
- DIVISION 9 — PRIVACY COMPLAINTS. **Section 36.**

Further details on the Access to Information and Protection of Privacy Act can be found at canlii.org.