Legislative Assembly of Ontario

Assemblée législative de l'Ontario

1ST SESSION, 43RD LEGISLATURE, ONTARIO
3 CHARLES III, 2024

# Bill 194

## An Act to enact the Enhancing Digital Security and Trust Act, 2024 and to make amendments to the Freedom of Information and Protection of Privacy Act respecting privacy protection measures

**The Hon. T. McCarthy**
Minister of Public and Business Service Delivery and Procurement

**Government Bill**

| | |
|---|---|
| 1st Reading | May 13, 2024 |
| 2nd Reading | October 29, 2024 |
| 3rd Reading | |
| Royal Assent | |

*(Reprinted as amended by the Standing Committee on Justice Policy and as reported to the Legislative Assembly November 25, 2024)*

*(The provisions in this bill will be renumbered after 3rd Reading)*

This reprint of the Bill is marked to indicate the changes that were made in Committee.

The changes are indicated by underlines for new text and a ~~strikethrough~~ for deleted text.

---

EXPLANATORY NOTE

**SCHEDULE 1**
**ENHANCING DIGITAL SECURITY AND TRUST ACT, 2024**

The Schedule enacts the *Enhancing Digital Security and Trust Act, 2024*.

The Act addresses cyber security and artificial intelligence systems at public sector entities. Public sector entities are the following: institutions within the meaning of the *Freedom of Information and Protection of Privacy Act*, other than the Assembly; ~~and~~ institutions within the meaning of the *Municipal Freedom of Information and Protection of Privacy Act*; children's aid societies and school boards.

Regulations may be made respecting cyber security at public sector entities, including regulations requiring them to develop and implement programs. Regulations may also set technical standards respecting cyber security.

Public sector entities may be required to comply with requirements respecting the use of artificial intelligence, including requirements to provide information, to develop and implement accountability frameworks and to take steps respecting risk management. In prescribed circumstances, they may be required to disclose information and ensure an individual provides oversight of the use of an artificial intelligence system. The regulations may also set technical standards respecting artificial intelligence systems.

The Act also addresses digital technology affecting individuals under age 18 as it relates to children's aid societies and school boards. Regulations may be made respecting the collection, use, retention and disclosure of digital information relating to individuals under age 18. Regulations may also set technical standards respecting this information and digital technology.

**SCHEDULE 2**
**FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT**

The Schedule amends the *Freedom of Information and Protection of Privacy Act*. Here are some highlights:

1. The definition of "information practices" is added to subsection 2 (1).
2. Section 34 is amended to, among other things, add a requirement for the annual report of a head of an institution to specify the number of thefts, losses or unauthorized uses or disclosures of personal information reported to the Commissioner during the year.
3. Section 38 is amended to add a requirement to assess various things before collecting personal information and to require the head of an institution to implement steps to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring and to mitigate the risks to individuals in the event of such an occurrence. A new subsection 38 (5) requires that assessments be updated before making any significant change to the purpose for which personal information is used or disclosed.
4. A new subsection 40 (5) requires the head of an institution to take steps to ensure that personal information in the custody or under the control of the institution is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.
5. A new section 40.1 requires that the head of an institution notify the Commissioner and the affected individual in the case of any theft, loss or unauthorized use or disclosure of the individual's personal information if there is a real risk of significant harm to the individual or if any other prescribed circumstances exist. Factors relevant to determining a real risk of significant harm are set out in subsection 40.1 (7).
6. A new section 49.0.1 authorizes the Commissioner to conduct a review of the information practices of an institution if the Commissioner has received a complaint under subsection 40.1 (4) or has other reason to believe that the requirements of Part III are not being complied with.
7. Subsection 55 (1) is amended to provide that information may be disclosed for a prescribed purpose.
8. A new section 57.1 requires the Commissioner to keep confidential the identity of a person who has notified the Commissioner of a contravention or potential contravention of the Act or regulations.
9. Subsection 58 (2) is amended to require that the Commissioner's annual report to the Speaker of the Assembly provide for the number of complaints received by the Commissioner in respect to the information practices of institutions and the number of reviews conducted under section 49.0.1

10. Section 59 is amended to authorize the Commissioner to, subject to some limitations, consult with a law enforcement officer or any person who, under an Act of Canada or of another province or territory of Canada, has powers, duties and functions similar to those of the Commissioner with respect to the protection of personal information.

11. Section 65.1 is amended to add more information to the definition of "customer service information" and to authorize a service provider organization that collects customer service information to, with the consent of the individual, retain and use the information for the purposes of providing any designated service to the individual.

**Bill 194** **2024**

# An Act to enact the Enhancing Digital Security and Trust Act, 2024 and to make amendments to the Freedom of Information and Protection of Privacy Act respecting privacy protection measures

**CONTENTS**



## Preamble

The Government of Ontario:

Recognizes the importance of cyber security in establishing trust in digital services delivered by the public sector.

Believes that cyber security in the public sector should be strengthened.

Believes that artificial intelligence systems in the public sector should be used in a responsible, transparent, accountable and secure manner that benefits the people of Ontario while protecting privacy.

Recognizes that digital information and technology related to children warrants special protection.

Recognizes the importance of protecting the privacy of the people of Ontario and the value of enhancing Ontario's privacy safeguards through increased transparency and independent oversight.

Therefore, His Majesty, by and with the advice and consent of the Legislative Assembly of the Province of Ontario, enacts as follows:

**Contents of this Act**

**1 This Act consists of this section, sections 2 and 3 and the Schedules to this Act.**

**Commencement**

**2 (1) Except as otherwise provided in this section, this Act comes into force on the day it receives Royal Assent.**

**(2) The Schedules to this Act come into force as provided in each Schedule.**

**(3) If a Schedule to this Act provides that any of its provisions are to come into force on a day to be named by proclamation of the Lieutenant Governor, a proclamation may apply to one or more of those provisions, and proclamations may be issued at different times with respect to any of those provisions.**

**Short title**

**3 The short title of this Act is the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*.**

# SCHEDULE 1
# ENHANCING DIGITAL SECURITY AND TRUST ACT, 2024

## CONTENTS



## INTERPRETATION

### Definitions

**1** (1) In this Act,

"artificial intelligence system" means,

(a) a machine-based system that, for explicit or implicit objectives, infers from the input it receives in order to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments, and

(b) such other systems as may be prescribed; ("système d'intelligence artificielle")

"children's aid society" means a society within the meaning of the *Child, Youth and Family Services Act, 2017*; ("société d'aide à l'enfance")

"cyber security" means the security, continuity, confidentiality, integrity and availability of digital information and the infrastructure housing and transmitting digital information, and includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and information from attack, damage or unauthorized access; ("cybersécurité")

~~"Minister" means the Minister of Public and Business Service Delivery or such other member of the Executive Council as may be designated under the *Executive Council Act* to administer this Act; ("ministre")~~

"Minister" means the Minister of Public and Business Service Delivery and Procurement or such other member of the Executive Council as may be designated under the *Executive Council Act* to administer this Act; ("ministre")

"prescribed" means prescribed by the regulations made under this Act; ("prescrit")

"public sector entity" means,

~~(a) an institution within the meaning of subsection 2 (1) of the *Freedom of Information and Protection of Privacy Act*,~~

(a) an institution within the meaning of subsection 2 (1) of the *Freedom of Information and Protection of Privacy Act*, other than the Assembly,

(b) an institution within the meaning of subsection 2 (1) of the *Municipal Freedom of Information and Protection of Privacy Act*,

(c) a children's aid society, and

(d) a school board; (“entité du secteur public”)

“school board” means a board as defined in subsection 1 (1) of the *Education Act*. (“conseil scolaire”)

**Artificial intelligence system**

(2) For greater certainty, for the purposes of this Act, use of an artificial intelligence system by a public sector entity includes use of a system that is,

(a) publicly available;

(b) developed or procured by the public sector entity; or

(c) developed by a third party on behalf of the public sector entity.

**Digital information**

(3) For greater certainty, for the purposes of this Act, the collection, use, retention or disclosure of digital information by a public sector entity includes collection, use, retention or disclosure of digital information by a third party on behalf of the public sector entity.

CYBER SECURITY

**Regulations made by Lieutenant Governor in Council**

**2** (1) The Lieutenant Governor in Council may make regulations governing cyber security at such public sector entities as may be prescribed, including,

(a) requiring public sector entities to develop and implement programs for ensuring cyber security;

(b) governing programs mentioned in clause (a), which may include prescribing elements to be included in the programs;

(c) requiring public sector entities to submit reports to the Minister or a specified individual in respect of incidents relating to cyber security, which may include different requirements in respect of different types of incidents;

(d) prescribing the form and frequency of reports.

**Regulations re programs**

(2) Without limiting the generality of clause (1) (b), a regulation made under that clause may require that a public sector entity’s program include,

(a) roles and responsibilities of specified individuals within the public sector entity relating to ensuring cyber security;

(b) reporting on the public sector entity’s progress with respect to ensuring cyber security;

(c) education and awareness measures respecting cyber security;

(d) response and recovery measures for incidents relating to cyber security; and

(e) oversight measures for implementation of the program.

**Minister’s regulations re standards**

**3** The Minister may make regulations setting technical standards that such public sector entities as may be prescribed by the Minister must conform to respecting cyber security.

**Minister’s directives**

**4** (1) The Minister may issue directives to public sector entities respecting cyber security.

**Same**

(2) A directive may be general or particular in its application, and may provide for different classes or categories.

**Status**

(3) Part III (Regulations) of the *Legislation Act, 2006* does not apply with respect to a directive.

**Compliance**

(4) A public sector entity to whom a directive is issued shall comply with the directive.

USE OF ARTIFICIAL INTELLIGENCE SYSTEMS

**Use, intended use**

**Application**

**5** (1) This section applies to such public sector entities as may be prescribed for the purposes of this section if they use or intend to use an artificial intelligence system in prescribed circumstances.

**Information to public**

(2) A public sector entity to which this section applies shall, in accordance with the regulations, provide information to the public about their use of the artificial intelligence system.

**Accountability framework**

(3) A public sector entity to which this section applies shall, in accordance with the regulations, develop and implement an accountability framework respecting their use of the artificial intelligence system.

**Risk management**

(4) A public sector entity to which this section applies shall take such steps as may be prescribed to manage risks associated with the use of the artificial intelligence system.

**Requirements**

(5) A public sector entity to which this section applies shall use the artificial intelligence system in accordance with any prescribed requirements.

**Prohibited use**

(6) A public sector entity to which this section applies shall not use an artificial intelligence system if the use is prohibited by the regulations.

**Specific uses**

**Application**

**6** (1) This section applies in respect of such public sector entities as may be prescribed for the purposes of this section.

**Obligations**

(2) A public sector entity to which this section applies shall, when using an artificial intelligence system in prescribed circumstances,

(a) disclose information, in accordance with the regulations, respecting the use of the artificial intelligence system; and

(b) ensure that an individual,

(i) exercises oversight of the use of the artificial intelligence system, in accordance with the regulations, and

(ii) provides additional information, in accordance with the regulations, respecting the use of the artificial intelligence system.

**Regulations made by Lieutenant Governor in Council**

**7** The Lieutenant Governor in Council may make regulations governing the use of artificial intelligence systems by public sector entities, including,

(a) prescribing public sector entities to whom section 5 or 6 applies;

(b) prescribing circumstances for the purposes of subsection 5 (1);

(c) governing the provision of information under subsection 5 (2), which may include,

(i) prescribing the manner in which information must be provided,

(ii) prescribing information that must be provided,

(iii) prescribing information that is not required to be provided,

(iv) specifying when information must be provided and updated,

(v) exempting public sector entities from the requirement to provide information in specified circumstances;

(d) governing the development of accountability frameworks under subsection 5 (3), which may include,

(i) prescribing the form and content of the accountability frameworks,

(ii) specifying when the accountability frameworks must be developed and updated,

(iii) prescribing roles and responsibilities of specified individuals under the accountability frameworks,

(iv) requiring documentation respecting the use of the artificial intelligence system, including documentation respecting different phases of its use, performance and monitoring;

(e) prescribing steps to be taken for the purposes of subsection 5 (4), including reporting and record-keeping;

(f) prescribing requirements for the purposes of subsection 5 (5), which may include requiring that an artificial intelligence system be used only for specified purposes;

(g) prohibiting, for the purposes of subsection 5 (6), the use of an artificial intelligence system;

(h) prescribing circumstances for the purposes of subsection 6 (2);

(i) governing the disclosure of information under clause 6 (2) (a), which may include,

(i) prescribing the manner in which information must be disclosed,

(ii) prescribing information that must be disclosed,

(iii) prescribing information that is not required to be disclosed,

(iv) specifying when information must be disclosed and updated,

(v) exempting entities from the requirement to disclose information in specified circumstances;

(j) governing the exercise of oversight for the purposes of subclause 6 (2) (b) (i);

(k) governing the provision of additional information for the purposes of subclause 6 (2) (b) (ii), which may include requiring the provision of information about how to make inquiries about the use of the artificial intelligence system.

**Minister's regulations re standards**

**8** The Minister may make regulations setting technical standards that such public sector entities as may be prescribed by the Minister must conform to in their use of artificial intelligence systems.

## DIGITAL TECHNOLOGY AFFECTING INDIVIDUALS UNDER AGE 18

**Regulations made by Lieutenant Governor in Council**

**9** The Lieutenant Governor in Council may make regulations respecting such children's aid societies and school boards as may be prescribed,

(a) requiring prescribed digital information relating to individuals under age 18 that is collected, used, retained or disclosed to be collected, used, retained and disclosed in a prescribed manner;

(b) requiring reports to be submitted to the Minister or a specified individual in respect of the collection, use, retention and disclosure of information mentioned in clause (a);

(c) prohibiting the collection, use, retention or disclosure of prescribed digital information relating to individuals under age 18, which may include prohibiting such activities in prescribed circumstances, for prescribed purposes or subject to prescribed conditions.

**Minister's regulations re standards**

**10** The Minister may make regulations setting technical standards that such children's aid societies and school boards as may be prescribed by the Minister must conform to respecting,

(a) the collection, use, retention and disclosure of digital information relating to individuals under age 18; and

(b) digital technology made available for use by individuals under age 18.

**Minister's directives**

**11** (1) The Minister may issue directives to children's aid societies and school boards respecting digital technology made available for use by individuals under age 18.

**Same**

(2) A directive may be general or particular in its application, and may provide for different classes or categories.

**Status**

(3) Part III (Regulations) of the *Legislation Act, 2006* does not apply with respect to a directive.

**Compliance**

(4) A children's aid society or school board to whom a directive is issued shall comply with the directive.

## GENERAL

**No establishment of private law duty of care**

**12** Nothing in the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*, this Act or any regulation made or directive issued under this Act establishes a private law duty of care owing to any person.

**Effect of failure to comply**

**13** Failure to comply with this Act or any regulation made or directive issued under this Act does not affect the validity of any policy, Act, regulation, directive, instrument or decision.

**Conflict, general**

**14** If a provision of this Act or the regulations made or directives issued under this Act conflicts with a provision of any other Act or regulation, the provision in the other Act or regulation prevails.

**Directives, conflict**

**15** In the event of a conflict between a requirement set out in a directive issued under this Act and a directive made by the Management Board of Cabinet, the requirement in the directive made by the Management Board of Cabinet prevails.

**Regulations, general**

**16** The Lieutenant Governor in Council may make regulations prescribing anything in this Act that is referred to as prescribed or otherwise dealt with in the regulations, other than anything in respect of which the Minister is given authority to make regulations or which is referred to as prescribed by the Minister.

## COMMENCEMENT AND SHORT TITLE

**Commencement**

**17 The Act set out in this Schedule comes into force on a day to be named by proclamation of the Lieutenant Governor.**

**Short title**

**18 The short title of the Act set out in this Schedule is the *Enhancing Digital Security and Trust Act, 2024*.**

## SCHEDULE 2
## FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

**1 Subsection 2 (1) of the *Freedom of Information and Protection of Privacy Act* is amended by adding the following definition:**

"information practices" means the practices and procedures of an institution for actions in relation to personal information, including,

(a) when, how and the purposes for which the institution collects, uses, modifies, discloses, retains or disposes of personal information, and

(b) the administrative, technical and physical safeguards and practices that the institution maintains with respect to protecting the information; ("pratiques relatives aux renseignements")

**2 (1) The French version of clause 15 (b) of the Act is amended by striking out "des renseignements confidentiels confiés à une institution par un autre gouvernement ou par l'un de ses organismes" at the end and substituting "des renseignements qu'une institution a reçus à titre confidentiel d'un autre gouvernement ou de l'un de ses organismes".**

**(2) The French version of clause 15 (c) of the Act is amended by striking out "des renseignements confidentiels confiés à une institution par une organisation internationale d'États ou l'une de leurs entités" at the end and substituting " des renseignements qu'une institution a reçus à titre confidentiel d'une organisation internationale d'États ou de l'une de ses entités".**

**3 (1) Subsection 34 (1) of the Act is repealed and the following substituted:**

**Annual report of head**

(1) A head shall provide to the Commissioner an annual report with respect to the previous calendar year in accordance with this section.

**(2) Subsection 34 (2) of the Act is amended by adding the following clause:**

(c.1) the number of thefts, losses or unauthorized uses or disclosures of personal information recorded under subsection 40.1 (8);

**(3) Section 34 of the Act is amended by adding the following subsection:**

**Form of report etc.**

(5) The annual report shall be provided no later than the date specified by the Commissioner, if any, and shall be in the form and manner as may be specified by the Commissioner.

**4 (1) Subsection 38 (1) of the Act is amended by striking out "section 39" and substituting "section 39 and subsection 40 (5)".**

**(2) Section 38 of the Act is amended by adding the following subsections:**

**Privacy impact assessment**

(3) Unless the regulations provide otherwise, before collecting personal information, the head of an institution shall ensure that a written assessment is prepared that contains the following information respecting any personal information that the institution intends to collect:

1. The purpose for which the personal information is intended to be collected, used and disclosed, as applicable, and an explanation of why the personal information is necessary to achieve the purpose.
2. The legal authority for the intended collection, use and disclosure of the personal information.
3. The types of personal information that is intended to be collected and, for each type of personal information collected, an indication of how the type of personal information is intended to be used or disclosed.
4. The sources of the personal information that is intended be collected.
5. The position titles of the officers, employees, consultants or agents of the institution who will have access to the personal information.
6. Any limitations or restrictions imposed on the collection, use or disclosure of the personal information.
7. The period of time that the personal information would be retained by the institution, in accordance with subsection 40 (1).
8. An explanation of the administrative, technical and physical safeguards and practices that would be used to protect the personal information in accordance with subsection 40 (5) and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information.
9. The steps to be taken by the institution,

i. to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and

ii. to mitigate the risks to individuals in the event of such an occurrence.

10. Such other information as may be prescribed.

**Risk mitigation**

(4) The head of an institution shall ensure that the steps mentioned in paragraph 9 of subsection (3) are implemented,

(a) before collecting the personal information mentioned in that subsection; or

(b) if it is not possible to implement the steps before collecting the personal information, within a reasonable time after collecting the information.

**Requirement to update**

(5) Unless the regulations provide otherwise, before making any significant change to the purpose for which personal information mentioned in subsection (3) is used or disclosed, the head of an institution shall,

(a) update the assessment prepared under subsection (3) to reflect the proposed change and to set out the proposed intended use or disclosure; and

(b) implement any additional steps identified under paragraph 9 of subsection (3).

**Copy to Commissioner**

(6) The head of an institution shall, on request, provide the Commissioner with access to, or a copy of, an assessment prepared under subsection (3) or updated under subsection (5).

**5 Section 40 of the Act is amended by adding the following subsection:**

**Privacy safeguards**

(5) The head of an institution shall take steps that are reasonable in the circumstances to ensure that personal information in the custody or under the control of the institution is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the personal information are protected against unauthorized copying, modification or disposal.

**6 The Act is amended by adding the following section:**

**Breach of privacy safeguards**

**40.1** (1) The head of an institution shall report to the Commissioner any theft, loss or unauthorized use or disclosure of personal information in the custody or under the control of the institution if it is reasonable in the circumstances to believe that there is real risk that a significant harm to an individual would result or if any other prescribed circumstances exist.

**Report requirements**

(2) The report mentioned in subsection (1) must contain the prescribed information and must be made in the prescribed form and manner as soon as feasible after the head determines that the theft, loss or unauthorized use or disclosure has occurred.

**Notification to individual**

(3) Unless otherwise prohibited by law, the head of an institution shall notify an individual of any theft, loss or unauthorized use or disclosure of the individual's personal information that is in the custody or under the control of the institution if it is reasonable in the circumstances to believe that there is a real risk of significant harm to the individual or if any other prescribed circumstances exist.

**Contents of notification**

(4) The notification mentioned in subsection (3) must contain a statement that the individual is entitled to make a complaint to the Commissioner and any other prescribed information and must be made in the prescribed form and manner as soon as feasible after the head determines that the theft, loss or unauthorized use or disclosure of personal information has occurred.

**Complaints — time limit**

(5) A complaint mentioned in subsection (4) must be made in writing and filed with the Commissioner within one year after the subject-matter of the complaint first came to the attention of the complainant or should reasonably have come to the attention of the complainant, whichever is the shorter.

**Extension of time limit**

(6) Despite subsection (5), a complaint may be filed with the Commissioner after the time limit set out in that subsection if,

(a) the Commissioner is satisfied that the significance of the matter warrants a time extension and that the time extension would not result in any prejudice to any person; or

(b) the time limit set out in subsection (5) presents a barrier, as defined in the *Accessibility for Ontarians with Disabilities Act, 2005*, to the complainant and the Commissioner is satisfied that the time extension is reasonably required in the circumstances to accommodate the complainant for the purpose of making the complaint.

**Real risk of significant harm — factors**

(7) The factors that are relevant to determining whether a theft, loss or unauthorized use or disclosure of personal information creates a real risk of significant harm to an individual include,

(a) the sensitivity of the personal information;

(b) the probability that the personal information has been, is being or will be misused;

(c) the availability of steps that the individual could take to,

(i) reduce the risk of the harm occurring, or

(ii) mitigate the harm should it occur;

(d) any direction, recommendation or guidance provided by the Commissioner pertaining to what constitutes a real risk of significant harm; and

(e) any other prescribed factor.

**Records**

(8) The head of an institution shall, in accordance with any prescribed requirements, keep and maintain a record of every theft, loss or unauthorized use or disclosure of personal information reported under subsection (1).

**Provision to Commissioner**

(9) The head of an institution shall, on request, provide the Commissioner with access to, or a copy of, the record.

**Definition**

(10) In 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.

**Regulations**

(11) The Lieutenant Governor in Council may make regulations respecting anything in this section that is referred to as being prescribed.

**7 The Act is amended by adding the following section:**

**Commissioner's review of information practices**

**49.0.1** (1) The Commissioner may conduct a review of the information practices of an institution if the Commissioner has received a complaint under subsection 40.1 (4) or has other reason to believe that the requirements of this Part are not being complied with.

**Informal dispute resolution**

(2) Before conducting a review, the Commissioner may try to resolve the matter through mediation, conciliation or any other informal means of dispute resolution that the Commissioner considers appropriate.

**No review**

(3) The Commissioner may decide not to conduct a review for whatever reason the Commissioner considers proper, including if satisfied that,

(a) the institution has responded adequately to the complaint;

(b) the complaint has been or could be more appropriately dealt with, initially or completely, by means of a procedure, other than a complaint under this Act;

(c) there is insufficient evidence to warrant a review;

(d) the complaint is trivial, frivolous or vexatious or is made in bad faith;

(e) the subject matter of the complaint is already the object of an ongoing review under this section; or

(f) the subject matter of the complaint has already been the subject of a review by the Commissioner.

**Conduct of review**

(4) In conducting a review referred to in subsection (1), the Commissioner shall review the institution's information practices to determine whether,

(a) there has been unauthorized collection, use, modification, disclosure, access to or retention of personal information collected under this Part; and

(b) the requirements under this Part, including requirements with respect to notice, retention, security and secure disposal, have been met.

**Duty to assist**

(5) The head and all officers, employees, consultants and agents of an institution shall co-operate with and assist the Commissioner in the conduct of a review, including using any data storage processing or retrieval device or system to produce a record required by the Commissioner in readable form.

**Powers of Commissioner**

(6) The Commissioner may require the production of such information and records that are relevant to the subject matter of the review and that are in the custody or under the control of an institution.

**Orders**

(7) If, after giving an opportunity to be heard to the head of the institution, the Commissioner determines that an information practice contravenes this Part, the Commissioner may order the head to do any of the following:

1. Discontinue the information practice.
2. Change the information practice as specified by the Commissioner.
3. Return, transfer or destroy personal information collected or retained under the information practice.
4. Implement a different information practice as specified by the Commissioner.
5. Make a recommendation in respect of how the information practice could be improved.

**Limit on certain orders**

(8) The Commissioner may order under subsection (5) no more than what is reasonably necessary to achieve compliance with this Part.

**Procedure**

(9) The *Statutory Powers Procedure Act* does not apply to a review conducted under this section.

**8 Subsection 50 (4) of the Act is amended by striking out "under section 49.12 or an order made by the Commissioner under that section" and substituting "under section 49.0.1 or 49.12 or an order made by the Commissioner under either of those sections".**

**9 Subsection 55 (1) of the Act is amended by striking out "any other Act" at the end and substituting "any other Act, unless the disclosure is permitted for a prescribed purpose".**

**10 The Act is amended by adding the following section:**

**Whistleblowing**

**57.1** (1) Any person who has reasonable grounds to believe that an institution, a ministry data integration unit under Part III.1 or a multi-sector data integration unit under Part III.1 has contravened or is about to contravene this Act or the regulations may notify the Commissioner of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.

**Confidentiality**

(2) The Commissioner must keep confidential the identity of a person who has notified the Commissioner under subsection (1) and to whom an assurance of confidentiality has been provided by the Commissioner.

**11 Subsection 58 (2) of the Act is amended by adding the following clause:**

(0.a) the number of complaints received by the Commissioner in respect to the information practices of institutions and the number of reviews conducted under section 49.0.1;

**12 (1) Clause 59 (b) of the Act is repealed.**

**(2) Section 59 of the Act is amended by adding the following subsections:**

**Consultations with other privacy commissioners**

(2) The Commissioner may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with a law enforcement officer or any person who, under an Act of Canada or of another province or territory of Canada, has powers, duties and functions similar to those of the Commissioner with respect to the protection of personal information.

**Agreements or arrangements**

(3) The Commissioner may enter into agreements or arrangements with any person referred to in subsection (2) in order to,

(a) coordinate the activities of their offices and the office of the Commissioner, including to provide for mechanisms for the handling of any complaint in which they are mutually interested;

(b) undertake and publish research or develop and publish guidelines or other documents related to the protection of personal information;

(c) develop model contracts or other documents related to the protection of personal information that is collected, used or disclosed interprovincially or internationally; and

(d) develop procedures for collecting and disclosing information referred to in subsection (4).

**Collection or disclosure of information**

(4) The Commissioner may, in accordance with any procedure established under clause (3) (d), disclose information, other than information described in section 12, 14 or 19 of the Act, to any person referred to in subsection (2) of this section or may collect information from any such person, if the information,

(a) could be relevant to an ongoing or potential investigation of a complaint, inquiry or audit under this Act or under an Act of Canada or of another province or territory of Canada that has objectives that are similar to this Act; or

(b) could assist the Commissioner or that person in the exercise of their powers or the performance of their duties or functions with respect to the protection of personal information.

**Purpose and confidentiality**

(5) The procedures referred to in clause (3) (d) must,

(a) restrict the use of the information to the purpose for which it was originally disclosed; and

(b) stipulate that the information be treated in a confidential manner and not be further disclosed for other purposes without the express consent of the Commissioner.

**13 Subsection 60 (1) of the Act is amended by adding the following clauses:**

(c.1) governing assessments under section 38, including prescribing information to be included in an assessment and providing for circumstances in which an assessment or an update is not required to be prepared;

. . . . .

(g.2) prescribing purposes for which disclosure is permitted under subsection 55 (1);

**14 Clause 61 (1) (a) of the Act is amended by striking out "disclose" and substituting "collect, use or disclose".**

**15 (1) The definition of "customer service information" in subsection 65.1 (2) of the Act is repealed and the following substituted:**

"customer service information" means, in relation to a service,

(a) the name, sex, gender identity, preferred language and date of birth of the individual to whom the service is to be provided,

(b) the address, email address and telephone number or other contact information of the individual to whom the service is to be provided and, if applicable, the person acting on behalf of that individual, and an indication of any accessibility or communication preferences,

(c) the transaction or receipt number, the order status, the shipping status, the product identification number and the product expiry date provided by the service provider organization in relation to the request for the service, as applicable,

(d) information relating to the payment of any fee,

(e) information relating to communications between the service provider organization in relation to the request for the service and the individual to whom the service is to be provided, and, if applicable, the person acting on behalf of that individual, and

(f) such other information as may be prescribed; ("renseignements liés au service à la clientèle")

**(2) Section 65.1 of the Act is amended by adding the following subsection:**

**Additional uses of customer service information**

(4.1) A service provider organization that collects customer service information under subsection (4) is authorized to retain and use the information, with the consent of the individual to whom the information relates, for the purposes of providing any designated service to the individual.

**(3) Clause 65.1 (9) (a) of the Act is amended by striking out "clause (d)" and substituting "clause (f)".**

**Commencement**

**16 (1) Except as otherwise provided in this section, this Schedule comes into force on the day the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* receives Royal Assent.**

**(2) Sections 1 to 14 come into force on a day to be named by proclamation of the Lieutenant Governor.**