The following table compares the Consumer Privacy Protection Act (CPPA) provisions in Bill C-11 (left hand column) with the equivalent provisions (if there are any) in the Personal Information Protection and Electronic Documents Act (PIPEDA) (right hand column).

The table was created as my own personal reference. It was done quickly, and has not been vetted, reviewed or revised. I am happy to share it ‘as is’, but please be aware that there may be errors or omissions.

Structurally, the table follows the order of provisions in the CPPA, with the equivalent PIPEDA provisions on the left. PIPEDA was very awkwardly drafted, and it requires much jumping around in the statute to find the equivalent provisions. In some cases, these are in the statute itself, and in other cases, they are found in Schedule I to the statute. Things labeled as “principle” or “clause” in the PIPEDA column are from Schedule I.

Some provisions of CPPA are entirely new. You can spot these because the corresponding space in the PIPEDA column is blank.

The CPPA is part of Bill C-11. There is a second part of this bill which establishes a new data tribunal. I have not included this part of the bill in the comparison table, since there is no basis for comparison.

I may update/revise this table in the future. Feel free to check back to see if there is a new version.

If you feel I have missed something and wish to provide feedback, you can reach me at tscassa@uottawa.ca

Teresa Scassa
Canada Research Chair in Information Law and Policy
University of Ottawa
<table>
<thead>
<tr>
<th>CPPA</th>
<th>PIPA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in the course of commercial activities</strong></td>
<td><strong>An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act</strong></td>
</tr>
<tr>
<td><strong>alternative format</strong>, with respect to personal information, means a format that allows an individual with a sensory disability to read or listen to the personal information. (support de substitution)</td>
<td><strong>alternative format</strong>, with respect to personal information, means a format that allows a person with a sensory disability to read or listen to the personal information. (support de substitution)**</td>
</tr>
<tr>
<td><strong>automated decision system</strong> means any technology that assists or replaces the judgement of human decision-makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets. (système décisionnel automatisé)</td>
<td><strong>breach of security safeguards</strong> means the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization’s security safeguards that are referred to in section 57 or from a failure to establish those safeguards. (atteinte aux mesures de sécurité)**</td>
</tr>
<tr>
<td><strong>business transaction</strong> includes (a) the purchase, sale or other acquisition or disposition of an organization or a part of an organization, or any of its assets; (b) the merger or amalgamation of two or more organizations; (c) the making of a loan or provision of other financing to an organization or a part of an organization; (d) the creating of a charge on, or the taking of a security interest in or a security on, any assets or securities of an organization; (e) the lease or licensing of any of an organization’s assets; and (f) any other prescribed arrangement between two or more organizations to conduct a business activity. (transaction commerciale)</td>
<td><strong>business transaction</strong> includes (a) the purchase, sale or other acquisition or disposition of an organization or a part of an organization, or any of its assets; (b) the merger or amalgamation of two or more organizations; (c) the making of a loan or provision of other financing to an organization or a part of an organization; (d) the creating of a charge on, or the taking of a security interest in or a security on, any assets or securities of an organization; (e) the lease or licensing of any of an organization’s assets; and (f) any other prescribed arrangement between two or more organizations to conduct a business activity. (transaction commerciale)**</td>
</tr>
<tr>
<td><strong>commercial activity</strong> means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, taking into account an organization’s objectives for carrying out the transaction, act or conduct, the context in which it takes place, the persons involved and its outcome. (activité commerciale)</td>
<td><strong>commercial activity</strong> means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.</td>
</tr>
<tr>
<td><strong>Commissioner</strong> means the Privacy Commissioner appointed under section 53 of the <em>Privacy Act</em>. (commissaire)</td>
<td><strong>Commissioner</strong> means the Privacy Commissioner appointed under section 53 of the <em>Privacy Act</em>. (commissaire)</td>
</tr>
<tr>
<td><strong>de-identify</strong> means to modify personal information — or create information from personal information — by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual. (dépersonnaliser)</td>
<td></td>
</tr>
<tr>
<td><strong>disposal</strong> means the permanent and irreversible deletion of personal information. (retrait)</td>
<td></td>
</tr>
</tbody>
</table>
| **federal work, undertaking or business** means any work, undertaking or business that is within the legislative authority of Parliament. It includes:  
(a) a work, undertaking or business that is operated or carried on for or in connection with navigation and shipping, whether inland or maritime, including the operation of ships and transportation by ship anywhere in Canada;  
(b) a railway, canal, telegraph or other work or undertaking that connects a province with another province, or that extends beyond the limits of a province;  
(c) a line of ships that connects a province with another province, or that extends beyond the limits of a province;  
(d) a ferry between a province and another province or between a province and a country other than Canada;  
(e) aerodromes, aircraft or a line of air transportation;  
(f) a radio broadcasting station;  
(g) a bank or an authorized foreign bank as defined in section 2 of the *Bank Act*;  
(h) a work that, although wholly situated within a province, is before or after its execution declared by Parliament to be for the general | **federal work, undertaking or business** means any work, undertaking or business that is within the legislative authority of Parliament. It includes:  
(a) a work, undertaking or business that is operated or carried on for or in connection with navigation and shipping, whether inland or maritime, including the operation of ships and transportation by ship anywhere in Canada;  
(b) a railway, canal, telegraph or other work or undertaking that connects a province with another province, or that extends beyond the limits of a province;  
(c) a line of ships that connects a province with another province, or that extends beyond the limits of a province;  
(d) a ferry between a province and another province or between a province and a country other than Canada;  
(e) aerodromes, aircraft or a line of air transportation;  
(f) a radio broadcasting station;  
(g) a bank or an authorized foreign bank as defined in section 2 of the *Bank Act*;  
(h) a work that, although wholly situated within a province, is before or after its execution declared by Parliament to be for the general |
Parliament to be for the general advantage of Canada or for the advantage of two or more provinces; (i) a work, undertaking or business outside the exclusive legislative authority of the legislatures of the provinces; and (j) a work, undertaking or business to which federal laws, within the meaning of section 2 of the Oceans Act, apply under section 20 of that Act and any regulations made under paragraph 26(1)(k) of that Act. (entreprises fédérales)

**Minister** means the member of the Queen’s Privy Council for Canada designated under section 3 or, if no member is designated, the Minister of Industry. (ministre)

**organization** includes an association, a partnership, a person or a trade union. (organisation)

**personal health information**, with respect to an individual, whether living or deceased, means (a) information concerning the physical or mental health of the individual; (b) information concerning any health service provided to the individual; (c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual; (d) information that is collected in the course of providing health services to the individual; or (e) information that is collected incidentally to the provision of health services to the individual. (renseignement personnel sur la santé)

**personal information** means information about an identifiable individual. (renseignement personnel)

**prescribed** means prescribed by regulation. (Version anglaise seulement)

**record** means any documentary material, regardless of medium or form. (document)

**personal information** means information about an identifiable individual. (renseignement personnel)

**prescribed** means prescribed by regulation. (Version anglaise seulement)

**record** includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or
**service provider** means an organization, including a parent corporation, subsidiary, affiliate, contractor or subcontractor, that provides services for or on behalf of another organization to assist the organization in fulfilling its purposes. *(fournisseur de services)*  

**Tribunal** means the Personal Information and Data Protection Tribunal established under section 4 of the *Personal Information and Data Protection Tribunal Act*. *(Tribunal)*  

3 The Governor in Council may, by order, designate any member of the Queen’s Privy Council for Canada to be the Minister for the purposes of this Act.  

4 The rights and recourses provided under this Act may be exercised *(a)* on behalf of a minor or an individual under any other legal incapacity by a person authorized by or under law to administer the affairs or property of that individual;  
   *(b)* on behalf of a deceased individual by a person authorized by or under law to administer the estate or succession of that individual, but only for the purpose of that administration; and  
   *(c)* on behalf of any other individual by any person authorized in writing to do so by the individual.  

5 The purpose of this Act is to establish — in an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information — rules to govern the protection of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.  

3 The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.  

**Application**  
6 *(1)* This Act applies to every organization in respect of personal information that *(a)* the organization collects, uses or discloses in the course of commercial activities; or  

4 *(1)* This Part applies to every organization in respect of personal information that
(b) is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

**For greater certainty**

(2) For greater certainty, this Act applies in respect of personal information

(a) that is collected, used or disclosed interprovincially or internationally by an organization; or

(b) that is collected, used or disclosed by an organization within a province, to the extent that the organization is not exempt from the application of this Act under an order made under paragraph 119(2)(b).

**Application**

(3) This Act also applies to an organization set out in column 1 of the schedule in respect of personal information set out in column 2.

**Limit**

(4) This Act does not apply to

(a) any government institution to which the *Privacy Act* applies;

(b) any individual in respect of personal information that the individual collects, uses or discloses solely for personal or domestic purposes;

(c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose; or

(d) any organization in respect of an individual’s personal information that the organization collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession; or

(e) any organization that is, under an order made under paragraph 119(2)(b), exempt from the application of this Act in respect of the collection, use or disclosure of personal information that occurs within a province in respect of which the order was made.

<table>
<thead>
<tr>
<th><strong>4.01</strong></th>
<th>This Part does not apply to an organization in respect of the business contact information of an individual that the organization collects, uses or discloses in the course of commercial activities; or</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>the organization collects, uses or discloses in the course of commercial activities; or</td>
</tr>
<tr>
<td>(b)</td>
<td>is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.</td>
</tr>
<tr>
<td>(1.1)</td>
<td>This Part applies to an organization set out in column 1 of Schedule 4 in respect of personal information set out in column 2.</td>
</tr>
<tr>
<td>(2)</td>
<td>This Part does not apply to</td>
</tr>
<tr>
<td>(a)</td>
<td>any government institution to which the <em>Privacy Act</em> applies;</td>
</tr>
<tr>
<td>(b)</td>
<td>any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or</td>
</tr>
<tr>
<td>(c)</td>
<td>any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.</td>
</tr>
</tbody>
</table>
| 7 (1) An organization is accountable for personal information that is under its control. | **4.1 Principle 1 — Accountability**  
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the following principles. |

(2) Personal information is under the control of the organization that decides to collect it and that determines the purposes for its collection, use or disclosure, regardless of whether the information is collected, used or disclosed by the organization itself or by a service provider on behalf of the organization.

| 8 (1) An organization must designate one or more individuals to be responsible for matters related to its obligations under this Act. It must provide the designated individual’s business contact information to any person who requests it.  
(2) The designation of an individual under subsection (1) does not relieve the organization of its obligations under this Act. | **4.1.1 Accountability**  
Accountability for the organization’s compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).  
**4.1.2** The identity of the individual(s) designated by the organization to oversee the organization’s compliance with the principles shall be made known upon request.  
**4.1.4** Organizations shall implement policies and practices to give effect to the principles, including  
(a) implementing procedures to protect personal information;  
(b) establishing procedures to receive and respond to complaints and inquiries;  
(c) training staff and communicating to staff information about the organization’s policies and practices; and  
(d) developing information to explain the organization’s policies and procedures. |

| **CPPA s. 9 (1) Every organization must implement a privacy management program that includes the PIPEDA, Schedule I, Principle 4.1.4** |

|  | **(a) implementing procedures to protect personal information;** |

|  | **(b) establishing procedures to receive and respond to complaints and inquiries;** |

|  | **(c) training staff and communicating to staff information about the organization’s policies and practices; and** |

|  | **(d) developing information to explain the organization’s policies and procedures.** |
organization’s policies, practices and procedures put in place to fulfil its obligations under this Act, including policies, practices and procedures respecting
(a) the protection of personal information;
(b) how requests for information and complaints are received and dealt with;
(c) the training and information provided to the organization’s staff respecting its policies, practices and procedures; and
(d) the development of materials to explain the organization’s policies and procedures put in place to fulfil its obligations under this Act.

(2) In developing its privacy management program, the organization must take into account the volume and sensitivity of the personal information under its control.

| Organizations shall implement policies and practices to give effect to the principles, including |
| (a) implementing procedures to protect personal information; |
| (b) establishing procedures to receive and respond to complaints and inquiries; |
| (c) training staff and communicating to staff information about the organization’s policies and practices; and |
| (d) developing information to explain the organization’s policies and procedures. |

10 An organization must, on request of the Commissioner, provide the Commissioner with access to the policies, practices and procedures that are included in its privacy management program.

11 (1) If an organization transfers personal information to a service provider, the organization must ensure, by contract or otherwise, that the service provider provides substantially the same protection of the personal information as that which the organization is required to provide under this Act.

(2) The obligations under this Part, other than those set out in sections 57 and 61, do not apply to a service provider in respect of personal information that is transferred to it. However, the service provider is subject to all of the obligations under this Part if it collects, uses or discloses that information for any purpose other than the purposes for which the information was transferred.

| 4.1.3 |
| An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. |

| CPPA s. 12 (1) |
| An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances. |

| PIPEDA s. 5(3) |
| An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. |
(2) The following factors must be taken into account in determining whether the purposes referred to in subsection (1) are appropriate:

(a) the sensitivity of the personal information;
(b) whether the purposes represent legitimate business needs of the organization;
(c) the effectiveness of the collection, use or disclosure in meeting the organization’s legitimate business needs;
(d) whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and
(e) whether the individual’s loss of privacy is proportionate to the benefits in light of any measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.

(3) An organization must determine at or before the time of the collection of any personal information each of the purposes for which the information is to be collected, used or disclosed and record those purposes.

(4) If the organization determines that the personal information it has collected is to be used or disclosed for a new purpose, the organization must record that new purpose before using or disclosing that information for the new purpose.

4.2 Principle 2 — Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.1 The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2 Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfill these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6 This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the
| 13 | The organization may collect only the personal information that is necessary for the purposes determined and recorded under subsection 12(3). |
| 14 (1) | An organization must not use or disclose personal information for a purpose other than a purpose determined and recorded under subsection 12(3), unless the organization obtains the individual’s valid consent before any use or disclosure for that other purpose. |
| 14 (2) | Despite subsection (1), an organization may (a) use personal information for a purpose other than a purpose determined and recorded under subsection 12(3) in any of the circumstances set out in sections 18, 20 and 21, subsections 22(1) and (2) and sections 23, 24, 26, 30, 41 and 51; or (b) disclose personal information for a purpose other than a purpose determined and recorded under subsection 12(3) in any of the circumstances set out |
| 4.4 Principle 4 — Limiting Collection | The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means. |
| 4.4.1 | Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8). |
| 4.4.2 | The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception. |
| 4.4.3 | This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3). |
| 4.5 Principle 5 — Limiting Use, Disclosure, and Retention | Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes. |
| 4.5.1 | Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1). |
| 4.5.4 | This principle is closely linked to the Consent principle (Clause 4.3), the Identifying... |
in subsections 22(1) and (2), sections 23 to 28, 31 to 37 and 39, subsection 40(3) and sections 42 and 43 to 51.

Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

| 15 (1) Unless this Act provides otherwise, an organization must obtain an individual’s valid consent for the collection, use or disclosure of the individual’s personal information. |
| 16.1 For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. |
| (2) The individual’s consent must be obtained at or before the time of the collection of the personal information or, if the information is to be used or disclosed for a purpose other than a purpose determined and recorded under subsection 12(3), before any use or disclosure of the information for that other purpose. |
| Schedule I |
| 4.3 Principle 3 - Consent |
| (3) The individual’s consent is valid only if, at or before the time that the organization seeks the individual’s consent, it provides the individual with the following information in plain language: |
| 4.3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or |
| (a) the purposes for the collection, use or disclosure of the personal information determined by the organization and recorded under subsection 12(3) or (4); |
| (b) the way in which the personal information is to be collected, used or disclosed; |
| (c) any reasonably foreseeable consequences of the collection, use or disclosure of the personal information; |
| (d) the specific type of personal information that is to be collected, used or disclosed; and |
| (e) the names of any third parties or types of third parties to which the organization may disclose the personal information. |
| (4) Consent must be expressly obtained, unless the organization establishes that it is appropriate to rely on an individual’s implied consent, taking into account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed. |

| 4.3.2 In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information. |
disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2 The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.4 The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual’s name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual’s request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a
company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6 The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7 Individuals can give consent in many ways. For example:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(c) consent may be given orally when information is collected over the telephone; or

(d) consent may be given at the time that individuals use a product or service.

CPPA s. 15(5) The organization must not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of their personal information beyond what is necessary to provide the product or service.

PIPEDA, Schedule I, clause 4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.
| 16 | An organization must not obtain or attempt to obtain an individual’s consent by providing false or misleading information or using deceptive or misleading practices. Any consent obtained under those circumstances is invalid. | **CPPA s. 17 (1)** | On giving reasonable notice to an organization, an individual may, at any time, subject to this Act, to federal or provincial law or to the reasonable terms of a contract, withdraw their consent in whole or in part. |
| | | | (2) On receiving the notice from the individual, the organization must inform the individual of the consequences of the withdrawal of their consent and, as soon as feasible after that, cease the collection, use or disclosure of the individual’s personal information in respect of which the consent was withdrawn. |
| | **Business Operations** | **Business activities** | **PIPEDA, Schedule I, clause 4.3.8** |
| 18 (1) | An organization may collect or use an individual’s personal information without their knowledge or consent if the collection or use is made for a business activity described in subsection (2) and (a) a reasonable person would expect such a collection or use for that activity; and (b) the personal information is not collected or used for the purpose of influencing the individual’s behaviour or decisions. | | An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal. |
| List of activities | (2) Subject to the regulations, the following activities are business activities for the purpose of subsection (1): (a) an activity that is necessary to provide or deliver a product or service that the individual has requested from the organization; (b) an activity that is carried out in the exercise of due diligence to prevent or reduce the organization’s commercial risk; (c) an activity that is necessary for the organization’s information, system or network security; (d) an activity that is necessary for the safety of a product or service that the organization provides or delivers; |
(e) an activity in the course of which obtaining the individual’s consent would be impracticable because the organization does not have a direct relationship with the individual; and
(f) any other prescribed activity.

19 An organization may transfer an individual’s personal information to a service provider without their knowledge or consent.

20 An organization may use an individual’s personal information without their knowledge or consent to de-identify the information.

21 An organization may use an individual’s personal information without their knowledge or consent for the organization’s internal research and development purposes, if the information is de-identified before it is used.

22 (1) Organizations that are parties to a prospective business transaction may use and disclose an individual’s personal information without their knowledge or consent if
(a) the information is de-identified before it is used or disclosed and remains so until the transaction is completed;
(b) the organizations have entered into an agreement that requires the organization that receives the information
(i) to use and disclose that information solely for purposes related to the transaction,
(ii) to protect the information by security safeguards appropriate to the sensitivity of the information, and
(iii) if the transaction does not proceed, to return the information to the organization that disclosed it, or dispose of it, within a reasonable time;
(c) the organizations comply with the terms of that agreement; and
(d) the information is necessary
(i) to determine whether to proceed with the transaction, and
(ii) if the determination is made to proceed with the transaction, to complete it.

Completed business transaction
(2) If the business transaction is completed, the organizations that are parties to the transaction may use and disclose the personal information referred to

7.2 (1) In addition to the circumstances set out in subsections 7(2) and (3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, organizations that are parties to a prospective business transaction may use and disclose personal information without the knowledge or consent of the individual if

(a) the organizations have entered into an agreement that requires the organization that receives the personal information
(i) to use and disclose that information solely for purposes related to the transaction,
(ii) to protect that information by security safeguards appropriate to the sensitivity of the information, and
(iii) if the transaction does not proceed, to return that information to the organization that disclosed it, or destroy it, within a reasonable time; and
(b) the personal information is necessary
(i) to determine whether to proceed with the transaction, and
in subsection (1) without the individual’s knowledge or consent if

(a) the organizations have entered into an agreement that requires each of them

(i) to use and disclose the information under its control solely for the purposes for which the information was collected or permitted to be used or disclosed before the transaction was completed,

(ii) to protect that information by security safeguards appropriate to the sensitivity of the information, and

(iii) to give effect to any withdrawal of consent made under subsection 17(1);

(b) the organizations comply with the terms of that agreement;

(c) the information is necessary for carrying on the business or activity that was the object of the transaction; and

(d) one of the parties notifies the individual, within a reasonable time after the transaction is completed, that the transaction has been completed and that their information has been disclosed under subsection (1).

**Exception**

(3) Subsections (1) and (2) do not apply to a business transaction of which the primary purpose or result is the purchase, sale or other acquisition or disposition, or lease, of personal information.

(ii) if the determination is made to proceed with the transaction, to complete it.

(2) In addition to the circumstances set out in subsections 7(2) and (3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, if the business transaction is completed, organizations that are parties to the transaction may use and disclose personal information, which was disclosed under subsection (1), without the knowledge or consent of the individual if

(a) the organizations have entered into an agreement that requires each of them

(i) to use and disclose the personal information under its control solely for the purposes for which the personal information was collected, permitted to be used or disclosed before the transaction was completed,

(ii) to protect that information by security safeguards appropriate to the sensitivity of the information, and

(iii) to give effect to any withdrawal of consent made under clause 4.3.8 of Schedule 1;

(b) the personal information is necessary for carrying on the business or activity that was the object of the transaction; and

(c) one of the parties notifies the individual, within a reasonable time after the transaction is completed, that the transaction has been completed and that their personal information has been disclosed under subsection (1).

(3) An organization shall comply with the terms of any agreement into which it enters under paragraph (1)(a) or (2)(a).

(4) Subsections (1) and (2) do not apply to a business transaction of which the primary purpose
<table>
<thead>
<tr>
<th>23</th>
<th>An organization may collect, use or disclose an individual’s personal information without their knowledge or consent if it was produced by the individual in the course of their employment, business or profession and the collection, use or disclosure is consistent with the purposes for which the information was produced.</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 (2)</td>
<td>For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if</td>
</tr>
<tr>
<td></td>
<td>(b.2) the information was produced by the individual in the course of their employment, business or profession and the use is consistent with the purposes for which the information was produced;</td>
</tr>
<tr>
<td>7.3</td>
<td>In addition to the circumstances set out in section 7, for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, a federal work, undertaking or business may collect, use and disclose personal information without the consent of the individual if</td>
</tr>
<tr>
<td></td>
<td>(e.2) of information that was produced by the individual in the course of their employment, business or profession and the disclosure is consistent with the purposes for which the information was produced;</td>
</tr>
<tr>
<td>24</td>
<td>An organization that operates a federal, work or business may collect, use or disclose an individual’s personal information without their consent if</td>
</tr>
<tr>
<td></td>
<td>(a) the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the organization and the individual in connection with the operation of a federal work, undertaking or business; and</td>
</tr>
<tr>
<td></td>
<td>(b) the organization has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes.</td>
</tr>
<tr>
<td>7.3</td>
<td>In addition to the circumstances set out in section 7, for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, a federal work, undertaking or business may collect, use and disclose personal information without the consent of the individual if</td>
</tr>
<tr>
<td></td>
<td>(a) the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the federal work, undertaking or business and the individual; and</td>
</tr>
<tr>
<td></td>
<td>(b) the federal work, undertaking or business has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>25</strong></td>
<td>An organization may disclose an individual’s personal information without their knowledge or consent to a lawyer or, in Quebec, a lawyer or notary, who is representing the organization.</td>
</tr>
<tr>
<td><strong>26</strong></td>
<td>An organization may collect, use or disclose an individual’s personal information without their knowledge or consent if the information is contained in a witness statement and the collection, use or disclosure is necessary to assess, process or settle an insurance claim.</td>
</tr>
<tr>
<td><strong>27 (1)</strong></td>
<td>An organization may disclose an individual’s personal information to another organization without the individual’s knowledge or consent if the disclosure is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the individual’s knowledge or consent would compromise the ability to prevent, detect or suppress the fraud.</td>
</tr>
<tr>
<td></td>
<td>(2) An organization may collect an individual’s personal information without their knowledge or consent if the information was disclosed to it under subsection (1).</td>
</tr>
<tr>
<td><strong>28</strong></td>
<td>An organization may disclose an individual’s personal information without their knowledge or consent for the purpose of collecting a debt owed by the individual to the organization.</td>
</tr>
<tr>
<td><strong>29 (1)</strong></td>
<td>An organization may collect an individual’s personal information without their knowledge or consent for the purpose of collecting a debt owed by the individual to the organization.</td>
</tr>
<tr>
<td>Consent (1)</td>
<td>Consent (2)</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>Consent if the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way.</td>
<td>An organization may collect personal information without the knowledge or consent of the individual only if</td>
</tr>
<tr>
<td>(2) An organization may use an individual’s personal information without their knowledge or consent if the information was collected under subsection (1).</td>
<td>(a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;</td>
</tr>
<tr>
<td>30 An organization may use an individual’s personal information without their knowledge or consent for the purpose of acting in respect of an emergency that threatens the life, health or security of any individual.</td>
<td>7 (2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if</td>
</tr>
<tr>
<td>(b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;</td>
<td></td>
</tr>
<tr>
<td>31 An organization may disclose an individual’s personal information without their knowledge or consent to a person who needs the information because of an emergency that threatens the life, health or security of any individual. If the individual whom the information is about is alive, the organization must inform that individual in writing without delay of the disclosure.</td>
<td>7 (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is</td>
</tr>
<tr>
<td>(e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;</td>
<td></td>
</tr>
<tr>
<td>32 An organization may disclose an individual’s personal information without their knowledge or consent if the disclosure is necessary to identify the individual who is injured, ill or deceased and is made to a government institution, a part of a government institution or the individual’s next of kin or authorized representative. If the individual is alive, the organization must inform them in writing without delay of the disclosure.</td>
<td>7 (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is</td>
</tr>
<tr>
<td>(d.4) necessary to identify the individual who is injured, ill or deceased, made to a government institution, a part of a government institution or the individual’s next of kin or authorized representative and, if the individual is alive, the organization informs that individual in writing without delay of the disclosure;</td>
<td></td>
</tr>
<tr>
<td>33 An organization may disclose an individual’s personal information without their knowledge or consent to a government institution or part of a</td>
<td>7 (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual.

<table>
<thead>
<tr>
<th>34</th>
<th>An organization may on its own initiative disclose an individual’s personal information without their knowledge or consent to a government institution, a part of a government institution or the individual’s next of kin or authorized representative if (a) the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse; (b) the disclosure is made solely for purposes related to preventing or investigating the abuse; and (c) it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse.</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>An organization may disclose an individual’s personal information without their knowledge or consent if (a) the disclosure is made for statistical purposes or for scholarly study or research purposes and those purposes cannot be achieved without disclosing the information; (b) it is impracticable to obtain consent; and (c) the organization informs the Commissioner of the disclosure before the information is disclosed.</td>
</tr>
</tbody>
</table>

without the knowledge or consent of the individual only if the disclosure is (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (iv) the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual;

| 7 (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (d.3) made on the initiative of the organization to a government institution, a part of a government institution or the individual’s next of kin or authorized representative and (i) the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse, (ii) the disclosure is made solely for purposes related to preventing or investigating the abuse, and (iii) it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse; |

7 (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the
| 36 | An organization may disclose an individual’s personal information without their knowledge or consent to an institution whose functions include the conservation of records of historic or archival importance, if the disclosure is made for the purpose of such conservation. |
| 37 | An organization may disclose an individual’s personal information without their knowledge or consent after the earlier of (a) 100 years after the record containing the information was created, and (b) 20 years after the death of the individual. |
| 38 | An organization may collect an individual’s personal information without their knowledge or consent if the collection is solely for journalistic, artistic or literary purposes. |
| 39 | An organization may disclose an individual’s personal information without their knowledge or consent if (a) the personal information is de-identified before the disclosure is made; (b) the disclosure is made to (i) a government institution or part of a government institution in Canada, (ii) a health care institution, post-secondary educational institution or public library in Canada, (iii) any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government |

| 7 (3) | For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation; |
| 7 (3) | For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (h) made after the earlier of (i) one hundred years after the record containing the information was created, and (ii) twenty years after the death of the individual whom the information is about; |
| 7 (1) | For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if (c) the collection is solely for journalistic, artistic or literary purposes; |
institution in Canada, to carry out a socially
beneficial purpose, or
(iv) any other prescribed entity; and
(c) the disclosure is made for a socially beneficial
purpose.

(2) For the purpose of this section, *socially
beneficial purpose* means a purpose related to
health, the provision or improvement of public
amenities or infrastructure, the protection of the
environment or any other prescribed purpose.

| 40 (1) | An organization may collect an individual’s personal information without their knowledge or consent if it is reasonable to expect that the collection with their knowledge or consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of federal or provincial law. |
| Use | An organization may use an individual’s personal information without their knowledge or consent if the information was collected under subsection (1). |
| Disclosure | An organization may disclose an individual’s personal information without their knowledge or consent if the disclosure is made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of federal or provincial law that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation. |

<p>| 7 (1) | For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if |
| (b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; |
| 7(2) | For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if |
| (d) it was collected under paragraph (1)(a), (b) or (e). |
| 7 (3) | For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is |
| (d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>41</td>
<td>An organization may use an individual’s personal information without their knowledge or consent if, in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of federal or provincial law or law of a foreign jurisdiction that has been, is being or is about to be committed and the information is used for the purpose of investigating that contravention.</td>
</tr>
<tr>
<td>7(2)</td>
<td>For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if (a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention.</td>
</tr>
<tr>
<td>42</td>
<td>An organization may disclose an individual’s personal information without their knowledge or consent if (a) the disclosure is made to the other organization, government institution or part of a government institution that was notified of a breach under subsection 59(1); and (b) the disclosure is made solely for the purposes of reducing the risk of harm to the individual that could result from the breach or mitigating that harm.</td>
</tr>
<tr>
<td>10.2 (3)</td>
<td>In addition to the circumstances set out in subsection 7(3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual if (a) the disclosure is made to the other organization, the government institution or the part of a government institution that was notified of the breach under subsection (1); and (b) the disclosure is made solely for the purposes of reducing the risk of harm to the individual that could result from the breach or mitigating that harm.</td>
</tr>
<tr>
<td>43</td>
<td>An organization may disclose an individual’s personal information without their knowledge or consent to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of administering federal or provincial law.</td>
</tr>
<tr>
<td>7 (3)</td>
<td>For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (c.1) made to a government institution or part of a government institution that has made a request for</td>
</tr>
</tbody>
</table>
An organization may disclose an individual’s personal information without their knowledge or consent to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of enforcing federal or provincial law or law of a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law.

An organization may on its own initiative disclose an individual’s personal information without their knowledge or consent to a government institution or a part of a government institution if the organization has reasonable grounds to believe that the information relates to a contravention of federal or provincial law or law of a foreign jurisdiction that has been, is being or is about to be committed.

An organization may disclose an individual’s personal information without their knowledge or consent to the government institution referred to in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section.

The information, identified its lawful authority to obtain the information and indicated that:

- (iii) the disclosure is requested for the purpose of administering any law of Canada or a province, or

An organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is:

- (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
- (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law,

An organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is:

- (d) made on the initiative of the organization to a government institution or a part of a government institution and the organization
- (i) has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

An organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is:

- (c.2) made to the government institution mentioned in section 7 of the *Proceeds of Crime
(Money Laundering) and Terrorist Financing Act

<table>
<thead>
<tr>
<th>Section</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>47 (1)</td>
<td>An organization may disclose an individual’s personal information without their knowledge or consent to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs.</td>
</tr>
<tr>
<td>Collection</td>
<td>(2) An organization may collect an individual’s personal information without their knowledge or consent for the purpose of making a disclosure under subsection (1).</td>
</tr>
<tr>
<td>Use</td>
<td>(3) An organization may use an individual’s personal information without their knowledge or consent if it was collected under subsection (2).</td>
</tr>
<tr>
<td>48 (1)</td>
<td>An organization may on its own initiative disclose an individual’s personal information without their knowledge or consent to a government institution or a part of a government institution if the organization suspects that the information relates to national security, the defence of Canada or the conduct of international affairs.</td>
</tr>
<tr>
<td>Collection</td>
<td>(2) An organization may collect an individual’s personal information without their knowledge or consent to a government institution or part of a government institution if the organization suspects that the information relates to national security, the defence of Canada or the conduct of international affairs.</td>
</tr>
</tbody>
</table>

7 (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
(d) made on the initiative of the organization to a government institution or a part of a government institution and the organization

7 (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if
(e) the collection is made for the purpose of making a disclosure

7 (2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if
(d) it was collected under paragraph (1)(a), (b) or (e).
consent for the purpose of making a disclosure under subsection (1).

**Use**

(3) An organization may use an individual’s personal information without their knowledge or consent if it was collected under subsection (2).

(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

7(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if

(d) it was collected under paragraph (1)(a), (b) or (e).

7 (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if

(e) the collection is made for the purpose of making a disclosure

(i) under subparagraph (3)(c.1)(i) or (d)(ii),

49 (1) An organization may collect an individual’s personal information without their knowledge or consent for the purpose of making a disclosure that is required by law.

**Use**

(2) An organization may use an individual’s personal information without their knowledge or consent if it was collected under subsection (1).

**Disclosure**

(3) An organization may disclose an individual’s personal information without their knowledge or consent if the disclosure is required by law.

7(2) (d) it was collected under paragraph (1)(a), (b) or (e).

7(3) (i) required by law.

50 An organization may disclose an individual’s personal information without their knowledge or consent if the disclosure is required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of procedure relating to the production of records.

7(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

(c) required to comply with a subpoena or warrant issued or an order made by a court, person
An organization may collect, use or disclose an individual’s personal information without their knowledge or consent if the personal information is publicly available and is specified by the regulations.

The following definitions apply in this section.

**access** means to program, execute programs on, communicate with, store data in, retrieve data from or otherwise make use of any resources, including data or programs of a computer system or a computer network. *(utiliser)*

**computer program** has the same meaning as in subsection 342.1(2) of the Criminal Code. *(programme d’ordinateur)*

**computer system** has the same meaning as in subsection 342.1(2) of the Criminal Code. *(ordinateur)*

**electronic address** means an address used in connection with

(a) an electronic mail account;
(b) an instant messaging account; or
(c) any similar account. *(adresse électronique)*

**Collection and use of electronic addresses**

(2) An organization is not authorized under any of sections 18, 23 and 26, subsection 29(1) and sections 30, 38, 41 and 51 to

(a) collect an individual’s electronic address without their knowledge or consent, if the address is collected by the use of a computer program that is designed or marketed primarily for use in generating or searching for, and collecting, electronic addresses; or

(b) use an individual’s electronic address without their knowledge or consent, if the address is collected by the use of a computer program described in paragraph (a).

**Accessing computer system to collect personal information, etc.**

(3) An organization is not authorized under any of sections 18, 23 and 26, subsection 29(1), sections 30 and 38, subsection 40(1) and sections 41 and 51 to

1(1) (d) the information is publicly available and is specified by the regulations; or

1(2) (c.1) it is publicly available and is specified by the regulations; or

1(3) (h.1) of information that is publicly available and is specified by the regulations; or

2 Paragraphs 1(1)(a) and (b.1) to (d) and (2)(a) to (c.1) and the exception set out in clause 4.3 of Schedule 1 do not apply in respect of

(a) the collection of an individual’s electronic address, if the address is collected by the use of a computer program that is designed or marketed primarily for use in generating or searching for, and collecting, electronic addresses; or
(a) collect an individual’s personal information without their knowledge or consent, through any means of telecommunication, if the information is collected by accessing a computer system or causing a computer system to be accessed in contravention of an Act of Parliament; or
(b) use an individual’s personal information without their knowledge or consent, if the information is collected in a manner described in paragraph (a).

Express consent
(4) Despite subsection 15(4), an organization is not to rely on an individual’s implied consent in respect of any collection of personal information described in paragraph (2)(a) or (3)(a) or any use of personal information described in paragraph (2)(b) or (3)(b).

53 An organization must not retain personal information for a period longer than necessary to
(a) fulfil the purposes for which the information was collected, used or disclosed; or
(b) comply with the requirements of this Act, of federal or provincial law or of the reasonable terms of a contract.
The organization must dispose of the information as soon as feasible after that period.

54 An organization that uses personal information to make a decision about an individual must retain the information for a sufficient period of time to permit the individual to make a request for access under section 63.

(b) the use of an individual’s electronic address, if the address is collected by the use of a computer program described in paragraph (a).

(3) Paragraphs 7(1)(a) to (d) and (2)(a) to (c.1) and the exception set out in clause 4.3 of Schedule 1 do not apply in respect of
(a) the collection of personal information, through any means of telecommunication, if the collection is made by accessing a computer system or causing a computer system to be accessed in contravention of an Act of Parliament; or
(b) the use of personal information that is collected in a manner described in paragraph (a).

4.5.2 Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3
Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

Disposal at individual’s request
55 (1) If an organization receives a written request from an individual to dispose of personal information that it has collected from the individual, the organization must, as soon as feasible, dispose of the information, unless
(a) disposing of the information would result in the disposal of personal information about another individual and the information is not severable; or

(b) there are other requirements of this Act, of federal or provincial law or of the reasonable terms of a contract that prevent it from doing so.

(2) An organization that refuses a request must inform the individual in writing of the refusal, setting out the reasons and any recourse that they may have under section 73 or subsection 82(1).

(3) If an organization disposes of personal information, it must, as soon as feasible, inform any service provider to which it has transferred the information of the individual’s request and obtain a confirmation from the service provider that the information has been disposed of.

### 56 (1) An organization must take reasonable steps to ensure that personal information under its control is as accurate, up-to-date and complete as is necessary to fulfil the purposes for which the information is collected, used or disclosed.

#### Extent of accuracy

(2) In determining the extent to which personal information must be accurate, complete and up-to-date, the organization must take into account the individual’s interests, including

(a) whether the information may be used to make a decision about the individual;

(b) whether the information is used on an ongoing basis; and

(c) whether the information is disclosed to third parties.

#### Routine updating

(3) An organization is not to routinely update personal information unless it is necessary to fulfil the purposes for which the information is collected, used or disclosed.

### 4.6 Principle 6 — Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2 An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

4.6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

### 57 (1) An organization must protect personal information through physical, organizational and technical safeguards.

### 4.7 Principle 7 — Safeguards
technological security safeguards. The level of protection provided by those safeguards must be proportionate to the sensitivity of the information.

(2) In addition to the sensitivity of the information, the organization must, in establishing its security safeguards, take into account the quantity, distribution, format and method of storage of the information.

(3) The security safeguards must protect personal information against, among other things, loss, theft and unauthorized access, disclosure, copying, use and modification.

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3 The methods of protection should include

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

(b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and

(c) technological measures, for example, the use of passwords and encryption.

4.7.4 Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

58 (1) An organization must report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

Report requirements

10.1 (1) An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.
The report must contain the prescribed information and must be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.

### Notification to individual

Unless otherwise prohibited by law, an organization must notify an individual of any breach of security safeguards involving the individual’s personal information under the organization’s control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

### Contents of notification

The notification must contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It must also contain any other prescribed information.

### Form and manner

The notification must be conspicuous and must be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it must be given indirectly in the prescribed form and manner.

### Time to give notification

The notification must be given as soon as feasible after the organization determines that the breach has occurred.

### Definition of significant harm

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.

### Real risk of significant harm — factors

The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include

- the sensitivity of the personal information involved in the breach;
- the probability that the personal information has been, is being or will be misused; and
- any other prescribed factor.
(b) the probability that the personal information has been, is being or will be misused; and  

(c) any other prescribed factor.

<table>
<thead>
<tr>
<th>59 (1) An organization that notifies an individual of a breach of security safeguards under subsection 58(3) must notify any other organization, a government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm, or if any of the prescribed conditions are satisfied.</th>
</tr>
</thead>
</table>
| **Time to give notification**  
(2) The notification must be given as soon as feasible after the organization determines that the breach has occurred. |
| 60 (1) An organization must, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control. |
| **Provision to Commissioner**  
(2) An organization must, on request, provide the Commissioner with access to, or a copy of, the record. |
| 61 If a service provider determines that any breach of security safeguards has occurred that involves personal information, it must as soon as feasible notify the organization that controls the personal information. |

**CPPA 62 (1)** An organization must make readily available, in plain language, information that explains the organization’s policies and practices put in place to fulfil its obligations under this Act.  

(2) In fulfilling its obligation under subsection (1), an organization must make the following information available:  

(a) a description of the type of personal information under the organization’s control;  

**PIPEDA 4.8 Principle 8 — Openness**  

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.  

4.8.1 Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an
(b) a general account of how the organization makes use of personal information, including how the organization applies the exceptions to the requirement to obtain consent under this Act;
(c) a general account of the organization’s use of any automated decision system to make predictions, recommendations or decisions about individuals that could have significant impacts on them;
(d) whether or not the organization carries out any international or interprovincial transfer or disclosure of personal information that may have reasonably foreseeable privacy implications;
(e) how an individual may make a request for disposal under section 55 or access under section 63; and
(f) the business contact information of the individual to whom complaints or requests for information may be made.

4.8.2 The information made available shall include
(a) the name or title, and the address, of the person who is accountable for the organization’s policies and practices and to whom complaints or inquiries can be forwarded;
(b) the means of gaining access to personal information held by the organization;
(c) a description of the type of personal information held by the organization, including a general account of its use;
(d) a copy of any brochures or other information that explain the organization’s policies, standards, or codes; and
(e) what personal information is made available to related organizations (e.g., subsidiaries).

4.9 Principle 9 — Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that
organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision and of how the personal information that was used to make the prediction, recommendation or decision was obtained. is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1 Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.3 In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

| 64 (1) | A request under section 63 must be made in writing. Assistance (2) An organization must assist any individual who informs the organization that they need assistance in preparing a request to the organization. |
| 8 (1) | A request under clause 4.9 of Schedule 1 must be made in writing. (2) An organization shall assist any individual who informs the organization that they need assistance in preparing a request to the organization. |
| 65 | An organization may require the individual to provide it with sufficient information to allow the organization to fulfil its obligations under section 63. 4.9.2 An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose. |
| 66 (1) | The information referred to in section 63 must be provided to the individual in plain language. 10 An organization shall give access to personal information in an alternative format to an |
| Sensory disability | individual with a sensory disability who has a right of access to personal information under this Part and who requests that it be transmitted in the alternative format if |
| (2) For the purpose of section 63, an organization must give access to personal information in an alternative format to an individual with a sensory disability who requests that it be transmitted in that format if |
| (a) a version of the information already exists in that format; or |
| (b) its conversion into that format is reasonable and necessary in order for the individual to be able to exercise rights under this Act. |
| Sensive medical information | |
| (3) An organization may choose to give an individual access to sensitive medical information through a medical practitioner. |

| 67 (1) An organization must respond to a request made under section 63 with due diligence and in any case no later than 30 days after the day on which the request was received. |
| Extension of time limit |
| (2) An organization may extend the time limit |
| (a) for a maximum of 30 days if |
| (i) meeting the time limit would unreasonably interfere with the activities of the organization, or |
| (ii) the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet; or |
| (b) for the period that is necessary in order to be able to convert the personal information into an alternative format. |

| 4.9.4 An organization shall respond to an individual’s request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided. |
| 8. (3) An organization shall respond to a request with due diligence and in any case not later than thirty days after receipt of the request. |
| (4) An organization may extend the time limit |
| (a) for a maximum of thirty days if |
| (i) meeting the time limit would unreasonably interfere with the activities of the organization, or |
| (ii) the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet; or |
| (b) for the period that is necessary in order to be able to convert the personal information into an alternative format. |

| Reasons |
| (3) An organization that responds within the time limit and refuses a request must inform the individual in writing of the refusal, setting out the reasons and any recourse that they may have under section 73 or subsection 82(1). |

| Deemed refusal |

| 4.9.4 An organization shall respond to an individual’s request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided. |
| 8. (3) An organization shall respond to a request with due diligence and in any case not later than thirty days after receipt of the request. |
| (4) An organization may extend the time limit |
| (a) for a maximum of thirty days if |
| (i) meeting the time limit would unreasonably interfere with the activities of the organization, or |
| (ii) the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet; or |
| (b) for the period that is necessary in order to be able to convert the personal information into an alternative format. |
(4) If the organization fails to respond within the time limit, the organization is deemed to have refused the request.

In either case, the organization shall, no later than thirty days after the date of the request, send a notice of extension to the individual, advising them of the new time limit, the reasons for extending the time limit and of their right to make a complaint to the Commissioner in respect of the extension.

(5) If the organization fails to respond within the time limit, the organization is deemed to have refused the request.

. . .

(7) An organization that responds within the time limit and refuses a request shall inform the individual in writing of the refusal, setting out the reasons and any recourse that they may have under this Part.

<table>
<thead>
<tr>
<th>68</th>
<th>An organization must not respond to the individual’s request made under section 63 at a cost unless (a) the organization has informed the individual of the approximate cost; (b) the cost to the individual is minimal; and (c) the individual has advised the organization that the request is not being withdrawn.</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.9.4</td>
<td>An organization shall respond to an individual’s request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.</td>
</tr>
</tbody>
</table>

8. (6) An organization may respond to an individual’s request at a cost to the individual only if

(a) the organization has informed the individual of the approximate cost; and

(b) the individual has advised the organization that the request is not being withdrawn.

<table>
<thead>
<tr>
<th>69</th>
<th>An organization that has personal information that is the subject of a request made under section 63 must retain the information for as long as is necessary to allow the individual to exhaust any recourse that they may have under this Act.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. (8)</td>
<td>Despite clause 4.5 of Schedule 1, an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>70</th>
<th>(1) Despite section 63, an organization must not give an individual access to personal information under that section if doing so would likely reveal personal information about another individual. However, if the information about the other</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>(1) Despite clause 4.9 of Schedule 1, an organization shall not give an individual access to personal information if doing so would likely reveal personal information about a third party. However, if the information about the third party</td>
</tr>
</tbody>
</table>

36
individual is severable from the information about the requester, the organization must sever the information about the other individual before giving the requester access.

**Limit**

(2) Subsection (1) does not apply if the other individual consents to the access or the requester needs the information because an individual’s life, health or security is threatened.

**Information related to certain exceptions to consent**

(3) An organization must comply with subsection (4) if an individual requests that the organization

(a) inform the individual about

(i) any disclosure to a government institution or a part of a government institution under section 44, 45 or 46, subsection 47(1) or 48(1) or section 50, or

(ii) the existence of any information that the organization has relating to a disclosure referred to in subparagraph (i), to a subpoena, warrant or order referred to in section 50 or to a request made by a government institution or a part of a government institution under section 44 or subsection 47(1); or

(b) give the individual access to the information referred to in subparagraph (a)(ii).

**Notification and response**

(4) An organization to which subsection (3) applies

(a) must, in writing and without delay, notify the institution or part concerned of the request made by the individual; and

(b) must not respond to the request before the earlier of

(i) the day on which it is notified under subsection (5), and

(ii) 30 days after the day on which the institution or part is notified.

**Objection**

(5) Within 30 days after the day on which it is notified under subsection (4), the institution or part must notify the organization of whether the institution or part objects to the organization complying with the request. The institution or part may object only if the institution or part is of the opinion that compliance with the request could reasonably be expected to be injurious to

<table>
<thead>
<tr>
<th>is severable from the record containing the information about the individual, the organization shall sever the information about the third party before giving the individual access.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Subsection (1) does not apply if the third party consents to the access or the individual needs the information because an individual’s life, health or security is threatened.</td>
</tr>
</tbody>
</table>
| (2.1) An organization shall comply with subsection (2.2) if an individual requests that the organization

(a) inform the individual about

(i) any disclosure of information to a government institution or a part of a government institution under paragraph 7(3)(c), subparagraph 7(3)(c.1)(i) or (ii) or paragraph 7(3)(c.2) or (d), or

(ii) the existence of any information that the organization has relating to a disclosure referred to in subparagraph (i), to a subpoena, warrant or order referred to in paragraph 7(3)(c) or to a request made by a government institution or a part of a government institution under subparagraph 7(3)(c.1)(i) or (ii); or

(b) give the individual access to the information referred to in subparagraph (a)(ii).

(2.2) An organization to which subsection (2.1) applies

(a) shall, in writing and without delay, notify the institution or part concerned of the request made by the individual; and

(b) shall not respond to the request before the earlier of

(i) the day on which it is notified under subsection (2.3), and
(a) national security, the defence of Canada or the conduct of international affairs;
(b) the detection, prevention or deterrence of money laundering or the financing of terrorist activities; or
(c) the enforcement of federal or provincial law or law of a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law.

Prohibition

(6) Despite section 63, if an organization is notified under subsection (5) that the institution or part objects to the organization complying with the request, the organization

(a) must refuse the request to the extent that it relates to paragraph (3)(a) or to information referred to in subparagraph (3)(a)(ii);
(b) must notify the Commissioner, in writing and without delay, of the refusal; and
(c) must not give the individual access to any information that the organization has relating to a disclosure to a government institution or a part of a government institution under section 44, 45 or 46, subsection 47(1) or 48(1) or section 50 or to a request made by a government institution or part of a government institution under section 44 or subsection 47(1); and
(d) must not provide to the individual the name of the government institution or part to which the disclosure was made or its type; and
(e) must not disclose to the individual the fact that the organization notified an institution or part under paragraph (4)(a), that the institution or part objects or that the Commissioner was notified under paragraph (b).

When access may be refused

(7) Despite section 63, an organization is not required to give access to personal information if

(a) the information is protected by solicitor-client privilege or the professional secrecy of advocates and notaries or by litigation privilege;
(b) to do so would reveal confidential commercial information;
(c) to do so could reasonably be expected to threaten the life or security of another individual;

(ii) thirty days after the day on which the institution or part was notified.

(2.3) Within thirty days after the day on which it is notified under subsection (2.2), the institution or part shall notify the organization whether or not the institution or part objects to the organization complying with the request. The institution or part may object only if the institution or part is of the opinion that compliance with the request could reasonably be expected to be injurious to

(a) national security, the defence of Canada or the conduct of international affairs;
(b) the enforcement of any law of Canada, a province or a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law.

(2.4) Despite clause 4.9 of Schedule 1, if an organization is notified under subsection (2.3) that the institution or part objects to the organization complying with the request, the organization

(a) shall refuse the request to the extent that it relates to paragraph (2.1)(a) or to information referred to in subparagraph (2.1)(a)(ii);
(b) shall notify the Commissioner, in writing and without delay, of the refusal; and
(c) shall not disclose to the individual

(i) any information that the organization has relating to a disclosure to a government institution or a part of a government institution under paragraph 7(3)(c), subparagraph 7(3)(c.1)(i) or (ii) or paragraph 7(3)(c.2) or (d) or to a request made by a government institution under either of those subparagraphs,
(d) the information was collected under subsection 40(1);
(e) the information was generated in the course of a formal dispute resolution process; or
(f) the information was created for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act* or in the course of an investigation into a disclosure under that Act.

However, in the circumstances described in paragraph (b) or (c), if giving access to the information would reveal confidential commercial information or could reasonably be expected to threaten the life or security of another individual, as the case may be, and that information is severable from any other information for which access is requested, the organization must give the individual access after severing.

**Limit**

(8) Subsection (7) does not apply if the individual needs the information because an individual’s life, health or security is threatened.

**Notice**

(9) If an organization decides not to give access to personal information in the circumstances set out in paragraph (7)(d), the organization must, in writing, notify the Commissioner, and must provide any information that the Commissioner may specify.

(ii) that the organization notified an institution or part under paragraph (2.2)(a) or the Commissioner under paragraph (b), or
(iii) that the institution or part objects.

(3) Despite the note that accompanies clause 4.9 of Schedule 1, an organization is not required to give access to personal information only if

(a) the information is protected by solicitor-client privilege or the professional secrecy of advocates and notaries or by litigation privilege;

(b) to do so would reveal confidential commercial information;

(c) to do so could reasonably be expected to threaten the life or security of another individual;

(c.1) the information was collected under paragraph 7(1)(b);

(d) the information was generated in the course of a formal dispute resolution process; or

(e) the information was created for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act* or in the course of an investigation into a disclosure under that Act.

However, in the circumstances described in paragraph (b) or (c), if giving access to the information would reveal confidential commercial information or could reasonably be expected to threaten the life or security of another individual, as the case may be, and that information is severable from the record containing any other information for which access is requested, the organization shall give the individual access after severing.
4.9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

### Principle 4.10 Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization’s compliance.

4.10.1 The individual accountable for an organization’s compliance is discussed in Clause 4.1.1.
| **4.10.1** | An organization must investigate any complaint that it receives and make any necessary changes to its policies, practices and procedures as a result of the investigation. |
| **4.10.2** | Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use. |

**4.10.3** Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

**4.10.4** An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

| **74** | An organization that de-identifies personal information must ensure that any technical and administrative measures applied to the information are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information. |
| **75** | An organization must not use de-identified information alone or in combination with other information to identify an individual, except in order to conduct testing of the effectiveness of security safeguards that the organization has put in place to protect the information. |

**76 (1)** For the purpose of this section and sections 77 to 81, entity includes any organization, regardless of whether it is an organization to which this Act applies, or a government institution.

**Code of practice**

(2) An entity may, in the manner provided by the regulations, apply to the Commissioner for approval of a code of practice that provides for substantially the same or greater protection of personal information as some or all of the protection provided under this Act.

**Approval by Commissioner**

| **24** | The Commissioner shall |
| | (c) encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with Divisions 1 and 1.1; and |
(3) The Commissioner may approve the code of practice if the Commissioner determines that the code meets the criteria set out in the regulations.

77 (1) An entity may, in the manner provided by the regulations, apply to the Commissioner for approval of a certification program that includes
(a) a code of practice that provides for substantially the same or greater protection of personal information as some or all of the protection provided under this Act;
(b) guidelines for interpreting and implementing the code of practice;
(c) a mechanism by which an entity that operates the program may certify that an organization is in compliance with the code of practice;
(d) a mechanism for the independent verification of an organization’s compliance with the code of practice;
(e) disciplinary measures for non-compliance with the code of practice by an organization, including the revocation of an organization’s certification; and
(f) anything else that is provided in the regulations.

Approval by Commissioner
(2) The Commissioner may approve the certification program if the Commissioner determines that the program meets the criteria set out in the regulations.

78 The Commissioner must respond in writing to an application under subsection 76(2) or 77(1) in the time specified in the regulations.

79 The Commissioner must make public a decision to approve a code of practice or certification program.

80 For greater certainty, compliance with the requirements of a code of practice or a certification program does not relieve an organization of its obligations under this Act.

81 The Commissioner may
(a) request that an entity that operates an approved certification program provide the Commissioner with information that relates to the program;
(b) cooperate with an entity that operates an approved certification program for the purpose of the exercise of the Commissioner’s powers and the
performance of the Commissioner’s duties and functions under this Act;
(c) in accordance with the regulations, recommend to an entity that operates an approved certification program that an organization’s certification be withdrawn, in the circumstances and according to the criteria set out in the regulations, if the Commissioner is of the opinion that the organization is not in compliance with the requirements of the program;
(d) disclose information to the Commissioner of Competition, under an agreement or arrangement entered into under section 115, that relates to an entity that operates an approved certification program or an organization that is certified under an approved certification program;
(e) in accordance with the regulations, revoke an approval of a certification program in the circumstances and according to the criteria set out in the regulations; or
(f) consult with federal government institutions respecting codes of practice or certification programs.

82 (1) An individual may file with the Commissioner a written complaint against an organization for contravening Part 1.

Commissioner may initiate complaint
(2) If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Act, the Commissioner may initiate a complaint in respect of the matter.

Time limit
(3) A complaint that results from the refusal to grant a request made under section 63 must be filed within six months, or any longer period that the Commissioner allows, after the refusal or after the expiry of the time limit for responding to the request, as the case may be.

Notice
(4) The Commissioner must give notice of a complaint to the organization against which the complaint was made, unless the Commissioner decides under subsection 83(2) not to carry out an investigation.

11 (1) An individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or 1.1 or for not following a recommendation set out in Schedule 1.

(2) If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter.

(3) A complaint that results from the refusal to grant a request under section 8 must be filed within six months, or any longer period that the Commissioner allows, after the refusal or after the expiry of the time limit for responding to the request, as the case may be.

(4) The Commissioner shall give notice of a complaint to the organization against which the complaint was made.
83 (1) The Commissioner must carry out an investigation in respect of a complaint, unless the Commissioner is of the opinion that
(a) the complainant should first exhaust grievance or review procedures otherwise reasonably available;
(b) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under any federal law, other than this Act, or provincial law;
(c) the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose; or
(d) the complaint raises an issue in respect of which a certification program that was approved by the Commissioner under subsection 77(2) applies and the organization is certified under that program.

Exception
(2) Despite subsection (1), the Commissioner is not required to carry out an investigation in respect of an act alleged in a complaint if the Commissioner is of the opinion that the act, if proved, would constitute a contravention of any of sections 6 to 9 of An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act or section 52.01 of the Competition Act or would constitute conduct that is reviewable under section 74.011 of that Act.

Notification
(3) The Commissioner must notify the complainant and the organization that the Commissioner will not investigate the complaint or any act alleged in the complaint and give reasons. However, if the decision is made for any of the reasons set out in subsection (2), the Commissioner must notify the complainant only.

Compelling reasons
(4) The Commissioner may reconsider a decision not to investigate under subsection (1) if the Commissioner is satisfied that the complainant has established that there are compelling reasons to investigate.

12 (1) The Commissioner shall conduct an investigation in respect of a complaint, unless the Commissioner is of the opinion that
(a) the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;
(b) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province; or
(c) the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose.

Exception
(2) Despite subsection (1), the Commissioner is not required to conduct an investigation in respect of an act alleged in a complaint if the Commissioner is of the opinion that the act, if proved, would constitute a contravention of any of sections 6 to 9 of An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act or section 52.01 of the Competition Act or would constitute conduct that is reviewable under section 74.011 of that Act.

Notification
(3) The Commissioner shall notify the complainant and the organization that the Commissioner will not investigate the complaint or any act alleged in the complaint and give reasons.

Compelling reasons
(4) The Commissioner may reconsider a decision not to investigate under subsection (1), if the Commissioner is satisfied that the complainant
<table>
<thead>
<tr>
<th>84</th>
<th>The Commissioner may attempt to resolve a complaint by means of a dispute resolution mechanism such as mediation and conciliation, unless an inquiry is being conducted in respect of the complaint.</th>
</tr>
</thead>
<tbody>
<tr>
<td>85</td>
<td>(1) The Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that (a) there is insufficient evidence to pursue the investigation; (b) the complaint is trivial, frivolous or vexatious or is made in bad faith; (c) the organization has provided a fair and reasonable response to the complaint; (d) the matter is already the object of an ongoing investigation or inquiry under this Act; (e) the matter has already been the subject of a report or decision by the Commissioner; (f) any of the circumstances referred to in paragraphs 83(1)(a) to (d) apply; (g) the matter is being or has already been addressed under a procedure referred to in paragraph 83(1)(a) or (b); or (h) the matter is the object of a compliance agreement entered into under subsection 86(1).</td>
</tr>
<tr>
<td>Other reason</td>
<td>(2) The Commissioner may discontinue an investigation in respect of an act alleged in a complaint if the Commissioner is of the opinion that the act, if proved, would constitute a contravention of any of sections 6 to 9 of An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act or section 52.01 of the Competition Act or would constitute conduct that is reviewable under section 74.011 of that Act.</td>
</tr>
<tr>
<td>12.1(2)</td>
<td>The Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation.</td>
</tr>
<tr>
<td>12.2(1)</td>
<td>The Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that (a) there is insufficient evidence to pursue the investigation; (b) the complaint is trivial, frivolous or vexatious or is made in bad faith; (c) the organization has provided a fair and reasonable response to the complaint; (c.1) the matter is the object of a compliance agreement entered into under subsection 17.1(1); (d) the matter is already the object of an ongoing investigation under this Part; (e) the matter has already been the subject of a report by the Commissioner; (f) any of the circumstances mentioned in paragraph 12(1)(a), (b) or (c) apply; or (g) the matter is being or has already been addressed under a procedure referred to in paragraph 12(1)(a) or (b).</td>
</tr>
<tr>
<td>(2)</td>
<td>The Commissioner may discontinue an investigation in respect of an act alleged in a complaint if the Commissioner is of the opinion that the act, if proved, would constitute a contravention of any of sections 6 to 9 of An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act or section 52.01 of the Competition Act or would constitute conduct that is reviewable under section 74.011 of that Act.</td>
</tr>
</tbody>
</table>
86 (1) If, in the course of an investigation, the Commissioner believes on reasonable grounds that an organization has committed, is about to commit or is likely to commit an act or omission that could constitute a contravention of Part 1, the Commissioner may enter into a compliance agreement with that organization, aimed at ensuring compliance with this Act.

**Terms**

(2) A compliance agreement may contain any terms that the Commissioner considers necessary to ensure compliance with this Act.

**Effect of compliance agreement**

(3) The Commissioner must not commence an inquiry under section 88 in respect of any matter covered under the agreement.

**For greater certainty**

(4) For greater certainty, a compliance agreement does not preclude the prosecution of an offence under this Act.

17.1 (1) If the Commissioner believes on reasonable grounds that an organization has committed, is about to commit or is likely to commit an act or omission that could constitute a contravention of a provision of Division 1 or 1.1 or a failure to follow a recommendation set out in Schedule 1, the Commissioner may enter into a compliance agreement, aimed at ensuring compliance with this Part, with that organization.

(2) A compliance agreement may contain any terms that the Commissioner considers necessary to ensure compliance with this Part.

(3) When a compliance agreement is entered into, the Commissioner, in respect of any matter covered under the agreement,

(a) shall not apply to the Court for a hearing under subsection 14(1) or paragraph 15(a); and

(b) shall apply to the court for the suspension of any pending applications that were made by the Commissioner under those provisions.

(4) For greater certainty, a compliance agreement does not preclude

(a) an individual from applying for a hearing under section 14; or

(b) the prosecution of an offence under the Act.

17.2 (1) If the Commissioner is of the opinion that a compliance agreement has been complied with, the Commissioner shall provide written notice to that effect to the organization and withdraw any applications that were made under
<table>
<thead>
<tr>
<th>Section</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>87</td>
<td>The Commissioner must notify the complainant and the organization and give reasons if an investigation has been discontinued or an investigation has concluded and the Commissioner will not be conducting an inquiry.</td>
</tr>
<tr>
<td>88 (1)</td>
<td>After investigating a complaint, the Commissioner may conduct an inquiry in respect of the complaint if the matter is not (a) the subject of dispute resolution under section 84; (b) discontinued; or (c) resolved. Notice (2) The Commissioner must give notice of the inquiry to the complainant and the organization.</td>
</tr>
<tr>
<td>89 (1)</td>
<td>If the Commissioner believes on reasonable grounds that an organization is not complying with the terms of a compliance agreement entered into under subsection 86(1), the Commissioner may conduct an inquiry in respect of the non-compliance. Notice (2) The Commissioner must give notice of the inquiry to the organization.</td>
</tr>
<tr>
<td>90 (1)</td>
<td>Subject to subsection (2), the Commissioner is not bound by any legal or technical rules of evidence in conducting an inquiry and must deal with the matter as informally and expeditiously as the circumstances and considerations of fairness and natural justice permit.</td>
</tr>
<tr>
<td>subsection 14(1) or paragraph 15(a)</td>
<td>in respect of any matter covered under the agreement.</td>
</tr>
<tr>
<td>12.2(3)</td>
<td>The Commissioner shall notify the complainant and the organization that the investigation has been discontinued and give reasons.</td>
</tr>
<tr>
<td>88 (1)</td>
<td>After investigating a complaint, the Commissioner may conduct an inquiry in respect of the complaint if the matter is not (a) the subject of dispute resolution under section 84; (b) discontinued; or (c) resolved. Notice (2) The Commissioner must give notice of the inquiry to the complainant and the organization.</td>
</tr>
<tr>
<td>89 (1)</td>
<td>If the Commissioner believes on reasonable grounds that an organization is not complying with the terms of a compliance agreement entered into under subsection 86(1), the Commissioner may conduct an inquiry in respect of the non-compliance. Notice (2) The Commissioner must give notice of the inquiry to the organization.</td>
</tr>
<tr>
<td>17.2 (2)</td>
<td>If the Commissioner is of the opinion that an organization is not complying with the terms of a compliance agreement, the Commissioner shall notify the organization and may apply to the Court for (a) an order requiring the organization to comply with the terms of the agreement, in addition to any other remedies it may give; or (b) a hearing under subsection 14(1) or paragraph 15(a) or to reinstate proceedings that have been suspended as a result of an application made under paragraph 17.1(3)(b). (3) Despite subsection 14(2), the application shall be made within one year after notification is sent or within any longer period that the Court may, either before or after the expiry of that year, allow.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Restriction</strong></td>
<td>(2) The Commissioner must not receive or accept as evidence anything that would be inadmissible in a court by reason of any privilege under the law of evidence.</td>
</tr>
<tr>
<td><strong>Opportunity to be heard</strong></td>
<td>(3) In conducting the inquiry, the Commissioner must give the organization and the complainant an opportunity to be heard and to be assisted or represented by counsel or by any person.</td>
</tr>
<tr>
<td><strong>Inquiry in private</strong></td>
<td>(4) The Commissioner may hold all or any part of the inquiry in private.</td>
</tr>
<tr>
<td><strong>91</strong></td>
<td>The Commissioner may determine the procedure to be followed in the conduct of an inquiry and must make that procedure publicly available.</td>
</tr>
<tr>
<td><strong>92</strong> (1)</td>
<td>The Commissioner must complete an inquiry by rendering a decision that sets out (a) the Commissioner’s findings on whether the organization has contravened this Act or has not complied with the terms of a compliance agreement; (b) any order made under subsection (2); (c) any decision made under subsection 93(1); and (d) the Commissioner’s reasons for the findings, order or decision.</td>
</tr>
<tr>
<td><strong>Compliance order</strong></td>
<td>(2) The Commissioner may, to the extent that is reasonably necessary to ensure compliance with this Act, order the organization to (a) take measures to comply with this Act; (b) stop doing something that is in contravention of this Act; (c) comply with the terms of a compliance agreement that has been entered into by the organization; or (d) make public any measures taken or proposed to be taken to correct the policies, practices or procedures that the organization has put in place to fulfil its obligations under this Act.</td>
</tr>
<tr>
<td><strong>Communication of decision</strong></td>
<td>(3) The decision must be sent to the complainant and the organization without delay.</td>
</tr>
<tr>
<td><strong>Extension of time</strong></td>
<td>(1) The Commissioner shall, within one year after the day on which a complaint is filed or is initiated by the Commissioner, prepare a report that contains (a) the Commissioner’s findings and recommendations; (b) any settlement that was reached by the parties; (c) if appropriate, a request that the organization give the Commissioner, within a specified time, notice of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken; and (d) the recourse, if any, that is available under section 14.</td>
</tr>
<tr>
<td></td>
<td>(2) [Repealed, 2010, c. 23, s. 84]</td>
</tr>
<tr>
<td></td>
<td>(3) The report shall be sent to the complainant and the organization without delay.</td>
</tr>
</tbody>
</table>
An inquiry conducted under section 88 must be completed within one year after the day on which the complaint is filed or is initiated by the Commissioner. However, the Commissioner may extend the time limit, for a period not exceeding one year, by notifying the complainant and the organization of the anticipated date on which the decision is to be made.

If, in completing an inquiry under section 88 or 89, the Commissioner finds that an organization has contravened one or more of the following provisions, the Commissioner must decide whether to recommend that a penalty be imposed on the organization by the Tribunal:

(a) section 13;
(b) subsection 14(1);
(c) subsection 15(5);
(d) section 16;
(e) section 53;
(f) subsections 55(1) and (3);
(g) subsection 57(1); and
(h) subsections 58(1) and (3).

Factors to consider
In making the decision, the Commissioner must take the following factors into account:
(a) the nature and scope of the contravention;
(b) whether the organization has voluntarily paid compensation to a person affected by the contravention;
(c) the organization’s history of compliance with this Act; and
(d) any other relevant factor.

Limitation
The Commissioner must not recommend that a penalty be imposed on an organization if the Commissioner is of the opinion that, at the time of the contravention of the provision in question, the organization was in compliance with the requirements of a certification program that was in relation to that provision and was approved by the Commissioner under subsection 77(2).

Notice to Tribunal
If the Commissioner decides to recommend that a penalty be imposed on an organization, the Commissioner must file with the Tribunal a copy of
the decision rendered under subsection 92(1) that sets out the decision to recommend.

94 (1) The Tribunal may, by order, impose a penalty on an organization if
(a) the Commissioner files a copy of a decision in relation to the organization in accordance with subsection 93(4) or the Tribunal, on appeal, substitutes its own decision to recommend that a penalty be imposed on the organization for the Commissioner’s decision not to recommend;
(b) the organization and the Commissioner are given the opportunity to make representations; and
(c) the Tribunal determines that imposing the penalty is appropriate.

Findings
(2) In determining whether it is appropriate to impose a penalty on an organization, the Tribunal must rely on the findings set out in the decision that is rendered by the Commissioner under subsection 92(1) in relation to the organization or on the Tribunal’s own findings if, on appeal, it substitutes its own findings for those of the Commissioner.

Limitations
(3) The Tribunal must not impose a penalty on an organization in relation to a contravention if a prosecution for the act or omission that constitutes the contravention has been instituted against the organization or if the organization establishes that it exercised due diligence to prevent the contravention.

Maximum penalty
(4) The maximum penalty for all the contraventions in a recommendation taken together is the higher of $10,000,000 and 3% of the organization’s gross global revenue in its financial year before the one in which the penalty is imposed.

Factors to consider
(5) In determining whether it is appropriate to impose a penalty on an organization and in determining the amount of a penalty, the Tribunal must take the following factors into account:
(a) the factors set out in subsection 93(2);
(b) the organization’s ability to pay the penalty and the likely effect of paying it on the organization’s ability to carry on its business; and
(c) any financial benefit that the organization obtained from the contravention.

**Purpose of penalty**

(6) The purpose of a penalty is to promote compliance with this Act and not to punish.

| 95 | A penalty imposed under section 94 constitutes a debt due to Her Majesty and the debt is payable and may be recovered by the Minister as of the day on which it is imposed. |
| 96 | The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization has contravened Part 1. [For procedures etc. see s. 98 below] |

| 18 (1) | The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization has contravened a provision of Division 1 or 1.1 or is not following a recommendation set out in Schedule 1, and for that purpose may |
| | (a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary for the audit, in the same manner and to the same extent as a superior court of record; |
| | (b) administer oaths; |
| | (c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law; |
| | (d) at any reasonable time, enter any premises, other than a dwelling-house, occupied by the organization on satisfying any security requirements of the organization relating to the premises; |
| | (e) converse in private with any person in any premises entered under paragraph (d) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and |
(f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the audit.

(2) The Commissioner may delegate any of the powers set out in subsection (1).

(3) The Commissioner or the delegate shall return to a person or an organization any record or thing they produced under this section within ten days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.

(4) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(d).

97 (1) After an audit, the Commissioner must provide the audited organization with a report that contains the findings of the audit and any recommendations that the Commissioner considers appropriate.

Reports may be included in annual reports
(2) The report may be included in a report made under section 118.

98 (1) In carrying out an investigation of a complaint, conducting an inquiry or carrying out an audit, the Commissioner may
(a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to carry out the investigation, conduct the inquiry or carry out the audit, in the same manner and to the same extent as a superior court of record;
(b) administer oaths;

19 (1) After an audit, the Commissioner shall provide the audited organization with a report that contains the findings of the audit and any recommendations that the Commissioner considers appropriate.

(2) The report may be included in a report made under section 25.

12.1 (1) In the conduct of an investigation of a complaint, the Commissioner may
(a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record;
(b) administer oaths;
(c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;
(d) make any interim order that the Commissioner considers appropriate;
(e) order an organization that has information that is relevant to the investigation, inquiry or audit to retain the information for as long as is necessary to allow the Commissioner to carry out the investigation, conduct the inquiry or carry out the audit;
(f) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises;
(g) converse in private with any person in any premises entered under paragraph (d) and otherwise make any inquiries in those premises that the Commissioner sees fit; and
(h) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the investigation.

Return of records
(2) The Commissioner or the Commissioner’s delegate must return to a person or an organization any record or thing that they produced under this section within 10 days after the day on which they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.

99 (1) The Commissioner may delegate any of the powers, duties or functions set out in sections 83 to 96 and subsection 98(1).

Certificate of delegation
(2) Any person to whom powers set out in subsection 98(1) are delegated must be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(d).

12.1 (3) The Commissioner may delegate any of the powers set out in subsection (1) or (2).
certificate of the delegation and the delegate must produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (f) of that subsection.

| 100 (1) | A complainant or organization that is affected by any of the following findings, orders or decisions may appeal it to the Tribunal:  
(a) a finding that is set out in a decision rendered under subsection 92(1);  
(b) an order made under subsection 92(2); or  
(c) a decision made under subsection 93(1) not to recommend that a penalty be imposed on the organization.  

**Time limit — appeal**  
(2) The time limit for making an appeal is 30 days after the day on which the Commissioner renders the decision under subsection 92(1) that sets out the finding, order or decision. |

| 101 (1) | A complainant or organization that is affected by an interim order made under paragraph 98(1)(d) may, with leave of the Tribunal, appeal the order to the Tribunal.  

**Time limit — leave to appeal**  
(2) The time limit for making an application for leave to appeal is 30 days after the day on which the order is made. |

| 102 (1) | The Tribunal may dispose of an appeal by dismissing it or by allowing it and, in allowing the appeal, the Tribunal may substitute its own finding, order or decision for the one under appeal.  

**Standard of review**  
(2) The standard of review for an appeal is correctness for questions of law and palpable and overriding error for questions of fact or questions of mixed law and fact. |

| 103 (1) | If an order made by the Commissioner under subsection 92(2) is not appealed to the Tribunal or an appeal of the order is dismissed by the Tribunal, the order may, for the purposes of its enforcement, be made an order of the Federal Court and is enforceable in the same manner as an order of that Court. |
**Interim orders**

(2) If an application for leave to appeal to the Tribunal is not made in relation to an order made by the Commissioner under paragraph 98(1)(d), a leave application in relation to the order is dismissed by the Tribunal or a leave application in relation to the order is granted by the Tribunal but the appeal is dismissed, then the order may, for the purposes of its enforcement, be made an order of the Federal Court and is enforceable in the same manner as an order of that Court.

---

**104** If the Tribunal, on appeal, substitutes its own order for an order of the Commissioner made under subsection 92(2) or paragraph 98(1)(d), the Tribunal’s order may, for the purposes of its enforcement, be made an order of the Federal Court and is enforceable in the same manner as an order of that Court.

**105** An order referred to in section 103 or 104 is made an order of the Federal Court by filing a certified copy of it with the Registrar of that Court.

**106 (1)** An individual who is affected by an act or omission by an organization that constitutes a contravention of this Act has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the contravention if

(a) the Commissioner has made a finding under paragraph 92(1)(a) that the organization has contravened this Act and

(i) the finding is not appealed and the time limit for making an appeal under subsection 100(2) has expired, or

(ii) the Tribunal has dismissed an appeal of the finding under subsection 102(1); or

(b) the Tribunal has made a finding under subsection 102(1) that the organization has contravened this Act.

**Damages — offence**

(2) If an organization has been convicted of an offence under section 125, an individual affected by the act or omission that gave rise to the offence has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the act or omission.
<table>
<thead>
<tr>
<th>Limitation period or prescription</th>
<th>Court of competent jurisdiction</th>
</tr>
</thead>
<tbody>
<tr>
<td>(3) An action must not be brought later than two years after the day on which the individual becomes aware of (a) in the case of an action under subsection (1), the Commissioner’s finding or, if there is an appeal, the Tribunal’s decision; and (b) in the case of an action under subsection (2), the conviction.</td>
<td>(4) An action referred to in subsection (1) or (2) may be brought in the Federal Court or a superior court of a province.</td>
</tr>
</tbody>
</table>

107 (1) If a certificate under section 38.13 of the *Canada Evidence Act* prohibiting the disclosure of personal information of a specific individual is issued before a complaint is filed by that individual under this Act in respect of a request for access to that information, the provisions of this Act respecting that individual’s right of access to their personal information do not apply to the information that is subject to the certificate.

**Certificate following filing of complaint**

(2) Despite any other provision of this Act, if a certificate under section 38.13 of the *Canada Evidence Act* prohibiting the disclosure of personal information of a specific individual is issued after the filing of a complaint under this Act in relation to a request for access to that information, (a) all proceedings under this Act in respect of that information, including an investigation, inquiry, audit, appeal or judicial review, are discontinued; (b) the Commissioner must not disclose the information and must take all necessary precautions to prevent its disclosure; and (c) the Commissioner must, within 10 days after the day on which the certificate is published in the *Canada Gazette*, return the information to the organization that provided the information.

(3) The Commissioner and every person acting on behalf or under the direction of the Commissioner, in exercising their powers and performing their duties and functions under this Act, must not disclose information subject to a certificate issued under section 38.13 of the *Canada Evidence Act* and must

4.1 (1) Where a certificate under section 38.13 of the *Canada Evidence Act* prohibiting the disclosure of personal information of a specific individual is issued before a complaint is filed by that individual under this Part in respect of a request for access to that information, the provisions of this Part respecting that individual’s right of access to his or her personal information do not apply to the information that is subject to the certificate.

(2) Notwithstanding any other provision of this Part, where a certificate under section 38.13 of the *Canada Evidence Act* prohibiting the disclosure of personal information of a specific individual is issued after the filing of a complaint under this Part in relation to a request for access to that information:

(a) all proceedings under this Part in respect of that information, including an investigation, audit, appeal or judicial review, are discontinued;

(b) the Commissioner shall not disclose the information and shall take all necessary precautions to prevent its disclosure; and

(c) the Commissioner shall, within 10 days after the certificate is published in the *Canada Gazette*, return the information to the organization that provided the information.
take every reasonable precaution to avoid the disclosure of that information.

**Power to delegate**

(4) The Commissioner must not delegate the investigation or inquiry in respect of any complaint relating to information subject to a certificate issued under section 38.13 of the *Canada Evidence Act* except to one of a maximum of four officers or employees of the Commissioner specifically designated by the Commissioner for the purpose of conducting that investigation or inquiry, as the case may be.

(3) The Commissioner and every person acting on behalf or under the direction of the Commissioner, in carrying out their functions under this Part, shall not disclose information subject to a certificate issued under section 38.13 of the *Canada Evidence Act*, and shall take every reasonable precaution to avoid the disclosure of that information.

(4) The Commissioner may not delegate the investigation of any complaint relating to information subject to a certificate issued under section 38.13 of the *Canada Evidence Act* except to one of a maximum of four officers or employees of the Commissioner specifically designated by the Commissioner for the purpose of conducting that investigation.

108 In addition to taking into account the purpose of this Act in the exercise of the Commissioner’s powers and the performance of the Commissioner’s duties and functions under this Act, the Commissioner must take into account the size and revenue of organizations, the volume and sensitivity of the personal information under their control and matters of general public interest.

109 The Commissioner must

(a) develop and conduct information programs to foster public understanding of this Act and recognition of its purposes;

(b) develop guidance materials for organizations in relation to their compliance with this Act — including any guidance materials that are requested by the Minister — in consultation with affected stakeholders, including any relevant federal government institutions;

(c) undertake and publish research that is related to the protection of personal information, including any research that is requested by the Minister;

(d) undertake and publish any research related to the operation or implementation of this Act that is requested by the Minister;

(e) on request by an organization, provide guidance on the organization’s privacy management program; and

24 The Commissioner shall

(a) develop and conduct information programs to foster public understanding, and recognition of the purposes, of this Part;

(b) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry;

(c) encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with Divisions 1 and 1.1; and

(d) promote, by any means that the Commissioner considers appropriate, the purposes of this Part.
(f) promote, by any other means that the Commissioner considers appropriate, the purposes of this Act.

| 110 | The Commissioner must not use the information they receive under section 10 or paragraph 109(e) as grounds to initiate a complaint under subsection 82(2) or to carry out an audit under section 96. |
| 111 | The Commissioner must make readily available information on the manner in which the Commissioner exercises the Commissioner’s powers or performs the Commissioner’s duties or functions under this Act. |

| 112 (1) Subject to subsections (3) to (8), section 79, paragraph 81(c), subsections 82(4) and 83(3), section 87, subsections 88(2) and 89(2), section 92, subsections 93(4), 97(1), 115(2), 116(3) and 117(1) and section 118, the Commissioner or any person acting on behalf or under the direction of the Commissioner must not disclose any information that comes to their knowledge as a result of the exercise of any of the Commissioner’s powers or the performance of any of the Commissioner’s duties or functions under this Act other than those referred to in subsection 58(1) or 60(2). |

**Confidentiality — reports and records**

| 20 (1) Subject to subsections (2) to (7), 12(3), 12.2(3), 13(3), 19(1), 23(3) and 23.1(1) and section 25, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge as a result of the performance or exercise of any of the Commissioner’s duties or powers under this Part other than those referred to in subsection 10.1(1) or 10.3(2). |

| (1.1) Subject to subsections (2) to (7), 12(3), 12.2(3), 13(3), 19(1), 23(3) and 23.1(1) and section 25, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information contained in a report made under subsection 10.1(1) or in a record obtained under subsection 10.3(2). |

| 2 | The Commissioner may, if the Commissioner considers that it is in the public interest to do so, make public any information that comes to his or her knowledge in the performance or exercise of any of his or her duties or powers under this Part. |

| 3 | The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information that in the Commissioner’s opinion is necessary to |

**Disclosure of necessary information**
The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information that in the Commissioner’s opinion is necessary to:

(a) carry out an investigation, conduct an inquiry or carry out an audit under this Act; or

(b) establish the grounds for findings and recommendations contained in any decision or report made under this Act.

### Disclosure in the course of proceedings

The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information in the course of:

(a) a prosecution for an offence under section 125;

(b) a prosecution for an offence under section 132 of the Criminal Code (perjury) in respect of a statement made under this Act;

(c) a proceeding or an appeal before the Tribunal under this Act; or

(d) a judicial review in relation to the exercise of any of the Commissioner’s powers or the performance of any of the Commissioner’s duties or functions under this Act or in relation to a decision of the Tribunal.

### Disclosure of offence authorized

The Commissioner may disclose to the Attorney General of Canada or of a province, as the case may be, information relating to the commission of an offence under any federal or provincial law on the part of an officer or employee of an organization if, in the Commissioner’s opinion, there is evidence of an offence.

### Disclosure of breach of security safeguards

The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, to a government institution or a part of a government institution, any information contained in a report made under subsection 58(1) or in a record obtained under subsection 60(2) if the Commissioner has reasonable grounds to believe that the information could be useful in the investigation of a contravention of any federal or provincial law that has been, is being or is about to be committed.
(8) The Commissioner may disclose information, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose information, in the course of proceedings in which the Commissioner has intervened under paragraph 50(c) of An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act or in accordance with subsection 58(3) or 60(1) of that Act.

(7) The Commissioner may disclose information, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose information, in the course of proceedings in which the Commissioner has intervened under paragraph 50(c) of An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act or in accordance with subsection 58(3) or 60(1) of that Act.

113 The Commissioner or any person acting on behalf or under the direction of the Commissioner is not a competent witness in respect of any matter that comes to their knowledge as a result of the exercise of any of the Commissioner’s powers or the performance of any of the Commissioner’s duties or functions under this Act in any proceeding other than (a) a prosecution for an offence under section 125; (b) a prosecution for an offence under section 132 of the Criminal Code (perjury) in respect of a statement made under this Act; or (c) a proceeding or an appeal before the Tribunal under this Act.

21 The Commissioner or person acting on behalf or under the direction of the Commissioner is not a competent witness in respect of any matter that comes to their knowledge as a result of the performance or exercise of any of the Commissioner’s duties or powers under this Part in any proceeding other than (a) a prosecution for an offence under section 28; (b) a prosecution for an offence under section 132 of the Criminal Code (perjury) in respect of a statement made under this Part; (c) a hearing before the Court under this Part; or (d) an appeal from a decision of the Court.

114 (1) No criminal or civil proceedings lie against the Commissioner, or against any person acting on behalf or under the direction of the Commissioner, for anything done, reported, decided or said in good faith as a result of the exercise or purported exercise of any power of the Commissioner or the performance or purported performance of any duty or function of the Commissioner under this Act.

22 (1) No criminal or civil proceedings lie against the Commissioner, or against any person acting on behalf or under the direction of the Commissioner, for anything done, reported or said in good faith as a result of the performance or exercise of any duty or power of the Commissioner under this Part.
<table>
<thead>
<tr>
<th>Defamation</th>
<th>(2) No action lies in defamation with respect to</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) No action lies in defamation with respect to</td>
<td>(a) anything said, any information supplied or any</td>
</tr>
<tr>
<td>(a) anything said, any information supplied or any record or thing</td>
<td>record or thing produced in good faith in the</td>
</tr>
<tr>
<td>produced in good faith in the course of an investigation or audit carried</td>
<td>course of an investigation or audit carried out</td>
</tr>
<tr>
<td>out or an inquiry conducted by or on behalf of the Commissioner under</td>
<td>by or on behalf of the Commissioner under this</td>
</tr>
<tr>
<td>this Act; and</td>
<td>Part; and</td>
</tr>
<tr>
<td>(b) any report or decision made in good faith by the Commissioner</td>
<td>(b) any report made in good faith by the</td>
</tr>
<tr>
<td>under this Act and any fair and accurate account of the report or</td>
<td>Commissioner under this Part and any fair and</td>
</tr>
<tr>
<td>decision made in good faith for the purpose of news reporting.</td>
<td>accurate account of the report made in good faith</td>
</tr>
<tr>
<td></td>
<td>for the purpose of news reporting.</td>
</tr>
<tr>
<td>115 (1) The Commissioner may enter into agreements or arrangements with the</td>
<td>Disclosure of information</td>
</tr>
<tr>
<td>Canadian Radio-television and Telecommunications Commission or the</td>
<td>(2) The Commissioner may, in accordance with any</td>
</tr>
<tr>
<td>Commissioner of Competition in order to</td>
<td>procedure established under paragraph (1)(b),</td>
</tr>
<tr>
<td>(a) undertake and publish research on issues of mutual interest; and</td>
<td>disclose information, other than information the</td>
</tr>
<tr>
<td>(b) develop procedures for disclosing information referred to in</td>
<td>Commissioner has received under section 10 or</td>
</tr>
<tr>
<td>subsection (2).</td>
<td>paragraph 109(e), to the Canadian Radio-television</td>
</tr>
<tr>
<td>Disclosure of information</td>
<td>and Telecommunications Commission or the</td>
</tr>
<tr>
<td>(2) The Commissioner may, in accordance with any procedure established</td>
<td>Commissioner of Competition if the information is</td>
</tr>
<tr>
<td>under paragraph (1)(b), disclose information, other than information</td>
<td>relevant to their powers, duties or functions.</td>
</tr>
<tr>
<td>the Commissioner has received under section 10 or paragraph 109(e),</td>
<td>Purpose and confidentiality</td>
</tr>
<tr>
<td>to the Canadian Radio-television and Telecommunications Commission or</td>
<td>(3) The procedures referred to in paragraph (1)(b)</td>
</tr>
<tr>
<td>the Commissioner of Competition if the information is relevant to their powers, duties or functions.</td>
<td></td>
</tr>
<tr>
<td>The procedures referred to in paragraph (1)(b) must</td>
<td>(a) restrict the use of the information to the</td>
</tr>
<tr>
<td>must</td>
<td>purpose for which it was originally disclosed; and</td>
</tr>
<tr>
<td>(a) restrict the use of the information to the purpose for which it was</td>
<td>(b) stipulate that the information be treated in a</td>
</tr>
<tr>
<td>originally disclosed; and</td>
<td>confidential manner and not be further disclosed</td>
</tr>
<tr>
<td>(b) stipulate that the information be treated in a confidential manner</td>
<td>without the express consent of the Commissioner.</td>
</tr>
<tr>
<td>and not be further disclosed without the express consent of the</td>
<td></td>
</tr>
<tr>
<td>Commissioner.</td>
<td></td>
</tr>
<tr>
<td>116 (1) If the Commissioner considers it appropriate to do so, or on the</td>
<td>23 (1) If the Commissioner considers it appropriate to do so, or on the request of an interested person, the Commissioner may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with any person who, under provincial legislation, has</td>
</tr>
<tr>
<td>request of an interested person, the Commissioner may, in order to</td>
<td></td>
</tr>
<tr>
<td>ensure that personal information is protected in as consistent a</td>
<td></td>
</tr>
<tr>
<td>manner as possible, consult with any person who, under provincial</td>
<td></td>
</tr>
<tr>
<td>legislation, has powers, duties and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
functions similar to those of the Commissioner with respect to the protection of personal information.

Agreements or arrangements with provinces
(2) The Commissioner may enter into agreements or arrangements with any person referred to in subsection (1) 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 disclosing information referred to in subsection (3).

Disclosure of information to provinces
(3) The Commissioner may, in accordance with any procedure established under paragraph (2)(d), disclose information, other than information the Commissioner has received under section 10 or paragraph 109(e), to any person referred to in subsection (1), if the information
(a) could be relevant to an ongoing or potential investigation of a complaint, inquiry or audit under this Act or provincial legislation 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
(4) The procedures referred to in paragraph (2)(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 without the express consent of the Commissioner.
(b) stipulate that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

117 (1) Subject to subsection (3), the Commissioner may, in accordance with any procedure established under paragraph (4)(b), disclose information referred to in subsection (2), other than information the Commissioner has received under section 10 or paragraph 109(e), that has come to the Commissioner’s knowledge as a result of the exercise of any of the Commissioner’s powers or the performance of any of the Commissioner’s duties and functions under this Act to any person or body who, under the legislation of a foreign state, has

(a) powers, duties and functions similar to those of the Commissioner with respect to the protection of personal information; or

(b) responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Act.

Information that can be disclosed

(2) The information that the Commissioner is authorized to disclose under subsection (1) is information that the Commissioner believes

(a) would be relevant to an ongoing or potential investigation or proceeding in respect of a contravention of the laws of a foreign state that address conduct that is substantially similar to conduct that would be in contravention of this Act; or

(b) is necessary to disclose in order to obtain from the person or body information that may be useful to an ongoing or potential investigation, inquiry or audit under this Act.

Written arrangements

(3) The Commissioner may only disclose information to the person or body referred to in subsection (1) if the Commissioner has entered into a written arrangement with that person or body that

(a) limits the information to be disclosed to that which is necessary for the purpose set out in paragraph (2)(a) or (b); and

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

23.1 (1) Subject to subsection (3), the Commissioner may, in accordance with any procedure established under paragraph (4)(b), disclose information referred to in subsection (2) that has come to the Commissioner’s knowledge as a result of the performance or exercise of any of the Commissioner’s duties or powers under this Part to any person or body who, under the legislation of a foreign state, has

(a) functions and duties similar to those of the Commissioner with respect to the protection of personal information; or

(b) responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Part.

(2) The information that the Commissioner is authorized to disclose under subsection (1) is information that the Commissioner believes

(a) would be relevant to an ongoing or potential investigation or proceeding in respect of a contravention of the laws of a foreign state that address conduct that is substantially similar to conduct that would be in contravention of this Part; or

(b) is necessary to disclose in order to obtain from the person or body information that may be useful to an ongoing or potential investigation or audit under this Part.

(3) The Commissioner may only disclose information to the person or body referred to in subsection (1) if the Commissioner has entered into a written arrangement with that person or body that
(c) stipulates that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

**Arrangements**

(4) The Commissioner may enter into arrangements with one or more persons or bodies referred to in subsection (1) in order to

(a) provide for cooperation with respect to the enforcement of laws protecting personal information, including the disclosure of information referred to in subsection (2) and the provision of mechanisms for the handling of any complaint in which they are mutually interested;

(b) establish procedures for disclosing information referred to in subsection (2);

(c) develop recommendations, resolutions, rules, standards or other documents with respect to the protection of personal information;

(d) undertake and publish research related to the protection of personal information;

(e) share knowledge and expertise by different means, including through staff exchanges; or

(f) identify issues of mutual interest and determine priorities pertaining to the protection of personal information.

(a) limits the information to be disclosed to that which is necessary for the purpose set out in paragraph (2)(a) or (b);

(b) restricts the use of the information to the purpose for which it was originally shared; and

(c) stipulates that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

(4) The Commissioner may enter into arrangements with one or more persons or bodies referred to in subsection (1) in order to

(a) provide for cooperation with respect to the enforcement of laws protecting personal information, including the sharing of information referred to in subsection (2) and the provision of mechanisms for the handling of any complaint in which they are mutually interested;

(b) establish procedures for sharing information referred to in subsection (2);

(c) develop recommendations, resolutions, rules, standards or other instruments with respect to the protection of personal information;

(d) undertake and publish research related to the protection of personal information;

(e) share knowledge and expertise by different means, including through staff exchanges; or

(f) identify issues of mutual interest and determine priorities pertaining to the protection of personal information.

118 (1) The Commissioner must, within three months after the end of each financial year, cause to be tabled in each House of Parliament a report concerning the application of this Act, the extent to which the provinces have enacted legislation that is

25 (1) The Commissioner shall, within three months after the end of each financial year, submit to Parliament a report concerning the application of this Part, the extent to which the provinces have enacted legislation that is substantially similar to
substantially similar to this Act and the application of any such legislation.

**Consultation**

(2) Before preparing the report, the Commissioner must consult with those persons in the provinces who, in the Commissioner’s opinion, are in a position to assist the Commissioner in making a report respecting personal information that is collected, used or disclosed interprovincially or internationally.

<table>
<thead>
<tr>
<th>119 (1) The Governor in Council may make regulations for carrying out the purposes and provisions of this Act, including regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) respecting the scope of any of the activities set out in paragraphs 18(2)(a) to (e), including specifying activities that are excluded from the activities set out in those paragraphs;</td>
</tr>
<tr>
<td>(b) specifying what is a government institution or part of a government institution for the purposes of any provision of this Act;</td>
</tr>
<tr>
<td>(c) specifying information for the purpose of section 51;</td>
</tr>
<tr>
<td>(d) specifying information to be kept and maintained under subsection 60(1); and</td>
</tr>
<tr>
<td>(e) prescribing anything that by this Act is to be prescribed.</td>
</tr>
</tbody>
</table>

**Orders**

(2) The Governor in Council may, by order,

(a) provide that this Act is binding on any agent of Her Majesty in right of Canada to which the Privacy Act does not apply;

(b) if satisfied that legislation of a province that is substantially similar to this Act applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Act in respect of the collection, use or disclosure of personal information that occurs within that province; and

(c) amend the schedule by adding or deleting, in column 1, a reference to an organization or by adding or deleting, in column 2, the description of personal information in relation to an organization in column 1.

**Regulations — substantially similar provincial legislation**

<table>
<thead>
<tr>
<th>26 (1) The Governor in Council may make regulations for carrying out the purposes and provisions of this Part, including regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) specifying, by name or by class, what is a government institution or part of a government institution for the purposes of any provision of this Part;</td>
</tr>
</tbody>
</table>

(a.01) [Repealed, 2015, c. 32, s. 21]

(a.1) specifying information or classes of information for the purpose of paragraph 7(1)(d), (2)(c.1) or (3)(h.1); |

(b) specifying information to be kept and maintained under subsection 10.3(1); and |

(c) prescribing anything that by this Part is to be prescribed. |

(2) The Governor in Council may, by order,

(a) provide that this Part is binding on any agent of Her Majesty in right of Canada to which the Privacy Act does not apply;

(b) if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province; and |
(3) The Governor in Council may make regulations establishing
(a) criteria that are to be applied in making a determination under paragraph (2)(b) that provincial legislation is substantially similar to this Act, or in reconsidering that determination; and
(b) the process for making or reconsidering that determination.

120 The Governor in Council may make regulations respecting the disclosure of personal information under section 72, including regulations
(a) respecting data mobility frameworks that provide for
(i) safeguards that must be put in place by organizations to enable the secure disclosure of personal information under section 72 and the collection of that information, and
(ii) parameters for the technical means for ensuring interoperability in respect of the disclosure and collection of that information;
(b) specifying organizations that are subject to a data mobility framework; and
(c) providing for exceptions to the requirement to disclose personal information under that section, including exceptions related to the protection of proprietary or confidential commercial information.

121 Regulations made under subsection 119(1) or section 120 may distinguish among different classes of activities, government institutions or parts of government institutions, information, organizations or entities.

122 The Minister may make regulations
(a) providing for the manner of making an application under subsection 76(2);
(b) setting out criteria for the purpose of subsection 76(3);
(c) respecting the reconsideration of a determination made under subsection 76(3);
(d) providing for the manner of making an application under subsection 77(1);
(e) providing for anything else that must be included in a certification program for the purpose of paragraph 77(1)(f);
(f) setting out criteria for the purpose of subsection 77(2);
(g) respecting the reconsideration of a determination made under subsection 77(2);
(h) specifying, for the purpose of section 78, the time for responding to an application;
(i) respecting the criteria for and the manner and the circumstances in which a recommendation may be made under paragraph 81(c);
(j) respecting the criteria for and the manner and the circumstances in which an approval may be revoked under paragraph 81(e); and
(k) respecting record-keeping and reporting obligations of an entity that operates an approved certification program, including obligations to provide reports to the Commissioner in respect of an approved certification program.

123 (1) Any person who has reasonable grounds to believe that a person has contravened or intends to contravene Part 1 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.

124 (1) An employer must not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee, or deny an employee a benefit of employment, by reason that
(a) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that the employer or any other person has contravened or intends to contravene Part 1;
(b) the employee, acting in good faith and on the basis of reasonable belief, has refused or stated an intention of refusing to do anything that is a contravention of Part 1;
(c) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an

27.1 (1) No employer shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee, or deny an employee a benefit of employment, by reason that
(a) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that the employer or any other person has contravened or intends to contravene a provision of Division 1 or 1.1;
(b) the employee, acting in good faith and on the basis of reasonable belief, has refused or stated an intention of refusing to do anything that is a contravention of a provision of Division 1 or 1.1;
intention of doing anything that is required to be done in order that Part 1 not be contravened; or
(d) the employer believes that the employee will do anything referred to in paragraph (a), (b) or (c).

Saving
(2) Nothing in this section impairs any right of an employee, either at law or under an employment contract or collective agreement.

Definitions of employee and employer
(3) In this section, employee includes an independent contractor and employer has a corresponding meaning.

| 125 | Every organization that knowingly contravenes section 58, subsection 60(1), section 69 or 75 or subsection 124(1) or an order under subsection 92(2) or that obstructs the Commissioner or the Commissioner’s delegate in the investigation of a complaint, in conducting an inquiry or in carrying out an audit is
(a) guilty of an indictable offence and liable to a fine not exceeding the higher of $25,000,000 and 5% of the organization’s gross global revenue in its financial year before the one in which the organization is sentenced; or
(b) guilty of an offence punishable on summary conviction and liable to a fine not exceeding the higher of $20,000,000 and 4% of the organization’s gross global revenue in its financial year before the one in which the organization is sentenced. |
| 28 | Every organization that knowingly contravenes subsection 8(8), section 10.1 or subsection 10.3(1) or 27.1(1) or that obstructs the Commissioner or the Commissioner’s delegate in the investigation of a complaint or in conducting an audit is guilty of
(a) an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or
(b) an indictable offence and liable to a fine not exceeding $100,000. |

| 126 | (1) Five years after the day on which this section comes into force, and every five years after that, a comprehensive review of the provisions and operation of this Act is to be commenced by a committee of the Senate, of the House of Commons or of both Houses of Parliament that may be designated or established by the Senate, the House of Commons or both Houses of Parliament, as the case may be, for that purpose.
Report |
| 29 | (1) The administration of this Part shall, every five years after this Part comes into force, be reviewed by the committee of the House of Commons, or of both Houses of Parliament, that may be designated or established by Parliament for that purpose.
(2) The committee shall undertake a review of the provisions and operation of this Part and shall, within a year after the review is undertaken or |
| (2) Within one year, or any further time that is authorized by the Senate, the House of Commons or both Houses of Parliament, as the case may be, after the day on which the review is commenced, the committee must submit a report on that review to the Senate, the House of Commons or both Houses of Parliament, as the case may be, together with a statement of any changes recommended by the committee. | within any further period that the House of Commons may authorize, submit a report to Parliament that includes a statement of any changes to this Part or its administration that the committee recommends. |