

# Comparative Table of Personal Information Protection Laws

---

AUGUST 2022






**FASKEN**

## Table of Contents

---

1.	Effective date.....	3	25.	Retention of information.....	19
2.	Responsible authority.....	3	26.	Statutory penalties.....	20
3.	Scope of application.....	4	27.	Remedies from regulatory authority.....	21
4.	Personal information (or “personal data”).....	4	28.	Private right of action.....	21
5.	Anonymized information.....	5	29.	Statutory certification programs.....	22
6.	De-identified information.....	5			
7.	Sensitive information.....	6			
8.	Consent.....	6			
9.	Exceptions to consent.....	7			
10.	Children.....	8			
11.	Governance program.....	9			
12.	Rights of access.....	9			
13.	Right to correct (or to rectify).....	11			
14.	Right to erasure (or “right to be forgotten”).....	11			
15.	Other rights of individuals.....	12			
16.	Privacy Officer.....	12			
17.	Transparency.....	13			
18.	Security measures.....	15			
19.	Breach definition.....	16			
20.	Breach notification.....	16			
21.	Transfer to foreign jurisdictions permitted.....	17			
22.	Privacy by design.....	18			
23.	New projects involving personal information.....	18			
24.	Audits.....	19			

# Comparative Table of Personal Information Protection Laws (Canada)

	 Canada	 Quebec	 Alberta	 British Columbia	 European Union	
	<i>Personal Information Protection and Electronic Documents Act</i> (PIPEDA) <sup>1</sup>	<i>Consumer Privacy Protection Act</i> (CPPA), as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act</i> (PIPA AB)	<i>BC Personal Information Protection Act</i> (PIPA BC)	<i>General Data Protection Regulation</i> (GDPR)
1. Effective date	<ul style="list-style-type: none"> <li>January 1, 2001 (applies to any organization since January 1, 2004)</li> </ul>	<ul style="list-style-type: none"> <li>Not in force</li> <li>Introduced by the Minister of Innovation, Science and Industry in the House of Commons on June 16, 2022</li> </ul>	<ul style="list-style-type: none"> <li>September 22, 2022: In particular, requirements for appointment of privacy officer, mandatory incident reporting and authorized transfer in cases of business transactions [exhaustive list of sections coming into force: 3.1; 3.5-3.8; 18; 18.4; 21-21.02; 46; 52; 56; 58; 61; 63-65; 67; 80; 80.1; 81.1-81.3; 83; 83.1; 86; 87; 90]<sup>4</sup></li> <li>September 22, 2023: Majority of provisions</li> <li>September 22, 2024: A form of right to “data portability”</li> </ul>	<ul style="list-style-type: none"> <li>January 1, 2004</li> </ul>	<ul style="list-style-type: none"> <li>January 1, 2004</li> </ul>	<ul style="list-style-type: none"> <li>May 25, 2018</li> </ul>
2. Responsible authority	<ul style="list-style-type: none"> <li>Office of the Privacy Commissioner of Canada (OPC) [2; 11]</li> </ul>	<ul style="list-style-type: none"> <li>Office of the Privacy Commissioner of Canada (OPC) [2; 76]</li> <li>Personal Information and Data Protection Tribunal<sup>5</sup></li> </ul>	<ul style="list-style-type: none"> <li>Commission d'accès à l'information du Québec (CAI) [41.1; 54]</li> </ul>	<ul style="list-style-type: none"> <li>Office of the Information and Privacy Commissioner of Alberta (OIPC AB) [36]</li> </ul>	<ul style="list-style-type: none"> <li>Office of the Information and Privacy Commissioner for British Columbia (OIPC BC) [36]</li> </ul>	<ul style="list-style-type: none"> <li>Supervisory authority of each Member State (CNIL in France, etc.) [51]</li> </ul>

1. On November 17, 2020, the Canadian government tabled substantial changes to Canadian privacy law in [Bill C-11, the Digital Charter Implementation Act, 2020](#) (C-11). C-11 Act proposed to (i) enact the *Consumer Privacy Protection Act* to replace Part 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which addresses privacy in the private sector; and (ii) enact the *Personal Information and Data Protection Tribunal Act* establishing the Personal Information and Data Protection Tribunal, which would hear recommendations of and appeals from decisions of the Privacy Commissioner of Canada (Commissioner). However, the dissolution of the government ended all work in progress in the Senate and in the House of Commons, including Bill C-11.

2. On June 16, 2022, the Canadian government tabled substantial changes to Canadian privacy law in [Bill C-27, the Digital Charter Implementation Act, 2022](#). In addition to enacting the CPPA and the Data Protection Tribunal Act (versions of which were proposed in the last federal privacy reform effort in November 2020), C-27 also proposes to enact the Artificial Intelligence and Data Act (AIDA) to regulate “artificial intelligence systems” and the processing of data in connection with artificial intelligence systems.

3. References made to this Act in the present column are references to the Act as amended by Bill 64 (also known as “Act 25”). To better identify the effective dates of the amendments, see [our version of the Act as amended by Bill 64](#).

4. The numbers in brackets refer to the section number of the referenced act.

5. Bill C-27 would also enact the Data Protection Tribunal Act, which would establish the Personal Information and Data Protection Tribunal.

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
<b>3. Scope of application</b>	<ul style="list-style-type: none"> <li>• Every organization that collects, uses or discloses personal information in the course of commercial activities in Canada or with a real and substantial connection to Canada<sup>6</sup> [4]</li> <li>• Excluding government institutions to which the Privacy Act applies [4(2)]</li> <li>• Possibility of exclusion from the application of PIPEDA in certain provinces (Alberta, BC and Québec) [26(2)]</li> <li>• Only covers employees of, or applicants for employment with, an organization that collects, uses or discloses personal information in connection with the operation of a federal work, undertaking or business [4(1)(b)]</li> </ul>	<ul style="list-style-type: none"> <li>• Every organization that collects, uses or discloses personal information in the course of commercial activities in Canada including: (1) interprovincially or internationally; or (2) within a province provided that the organization is not subject to an order under the CPPA stating that the organization is subject to provincial legislation that is substantially similar to the CPPA[6(1)(2); 122(1)]</li> <li>• Excluding government institutions to which the Privacy Act applies [6(4)(a)]</li> <li>• Possibility of exclusion from the application of CPPA in certain provinces having a “substantially similar law” (Alberta, BC and Québec private sector laws; Ontario, New Brunswick, Newfoundland and Labrador and Nova Scotia health information laws) [6(4)(e)]</li> </ul>	<ul style="list-style-type: none"> <li>• Any “enterprise” which collects, holds, uses or communicates personal information, whether the information is kept by the enterprise or through the agency of a third person [1]</li> <li>• Excluding public bodies within the meaning of the <i>Act respecting Access to documents held by public bodies and the Protection of personal information</i> [3]</li> </ul>	<ul style="list-style-type: none"> <li>• Any organization that collects, uses or discloses personal information [3]</li> <li>• Excluding “health information” to which the <i>Health Information Act</i> (Alberta) applies [4(3)]</li> <li>• Excluding personal information to which the <i>Freedom of Information and Protection of Privacy Act</i> (Alberta) applies (i.e., Alberta provincial public bodies) [4(3)]</li> </ul>	<ul style="list-style-type: none"> <li>• Any organization that collects, uses, or discloses personal information [2]</li> <li>• Excludes personal information to which PIPEDA applies</li> <li>• Excludes personal information to which the <i>Freedom of Information and Protection of Privacy Act</i> (BC) applies (i.e., BC provincial public bodies) [3]</li> </ul>	<ul style="list-style-type: none"> <li>• Establishment criterion: the controller or processor shall be established in the EU/EEA [3(1)]</li> <li>• Targeting criterion: the controller is established outside the EU/EEA but its processing activities are related to the offering of goods or services to individuals concerned in the EU/EEA or are related to the monitoring of the behaviour of individuals concerned in the EU/EEA [3(2)]</li> <li>• No distinction between the private and public sectors [4(7)]</li> </ul>
<b>4. Personal information (or “personal data”)</b>	<ul style="list-style-type: none"> <li>• Any information about an identifiable individual [2]</li> <li>• Whatever the physical form or characteristics</li> <li>• Particular regime for “business contact information” (information that is used for the purpose of communicating or facilitating communication with an individual in</li> </ul>	<ul style="list-style-type: none"> <li>• Any information about an identifiable individual [2]</li> <li>• Whatever the physical form or characteristics</li> <li>• “Personal information that the organization collects, uses or discloses <i>solely</i> for the purpose of communicating or facilitating communication with the individual</li> </ul>	<ul style="list-style-type: none"> <li>• Any information which relates to a natural person and allows that person to be identified, directly or indirectly [2]</li> <li>• Whatever the nature of its medium and whatever the form (written, graphic, taped, filmed, computerized, or other)</li> </ul>	<ul style="list-style-type: none"> <li>• Any information about an identifiable individual [1(1)(k)], including “personal employee information”</li> <li>• Excludes “business contact information” collected, used or disclosed for the purpose of enabling an</li> </ul>	<ul style="list-style-type: none"> <li>• Any information about an identifiable individual, including “employees’ personal information” [1]</li> <li>• Excludes “contact information” and “work product information” [1]</li> </ul>	<ul style="list-style-type: none"> <li>• Any information relating to an identified or identifiable natural person (including a name, an identification number, location data, an online identifier or a factor specific to the physical, physiological, genetic, mental, economic, cultural or social identity) [4(1)]</li> </ul>

6. Canadian courts apply the “real and substantial connection” test to determine when Canadian courts may take jurisdiction, and in practice Commissioners have taken jurisdiction and applied Canadian privacy law where there are relatively minimal connecting factors to Canada.

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
	relation to their employment, i.e., name, position, title, work address, professional phone number, etc.) [4.01]	in relation to their employment, business or profession” is excluded from the scope of the CPPA [6(4)(d)]	<ul style="list-style-type: none"> <li>Also covers employees and job applicants</li> <li>Particular regime for “personal information concerning the performance of duties within an enterprise by the person concerned, such as the person’s name, title and duties, as well as the address, email address and telephone number of the person’s place of work” [1]</li> </ul>	individual to be contacted in relation to the individual’s business responsibilities [4(3)]		<ul style="list-style-type: none"> <li>Whatever the medium/format</li> </ul>
<b>5. Anonymized information</b>	<ul style="list-style-type: none"> <li>No definition for anonymized information</li> <li>However, anonymization provided as an alternative to destruction or erasure of personal information when it is no longer required [Sch.1 - 4.5.3]</li> </ul>	<ul style="list-style-type: none"> <li>Information is considered anonymized when it irreversibly no longer allows the person to be identified directly or indirectly [2]</li> <li>Anonymization must be made according to generally accepted best practices [2]</li> <li>Dispose means permanently and irreversibly deleting personal information or <u>anonymizing it</u> [2]</li> <li>The CPPA does not apply to personal information that has been anonymized [6(5)]</li> </ul>	<ul style="list-style-type: none"> <li>Information is considered anonymized when it irreversibly no longer allows the person to be identified directly or indirectly [23]</li> <li>Anonymization must be made according to generally accepted best practices [23]</li> <li>Anonymization provided as an alternative to destruction of personal information when the purposes for which it was collected or used are achieved, provided that such anonymized information is used for serious and legitimate purpose [23]</li> </ul>	<ul style="list-style-type: none"> <li>No specific provision</li> </ul>	<ul style="list-style-type: none"> <li>No specific provision</li> </ul>	<ul style="list-style-type: none"> <li>Personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable; which processing is not subject to GDPR [recital 26]</li> </ul>
<b>6. De-identified information</b>	<ul style="list-style-type: none"> <li>No definition of “de-identified information”</li> </ul>	<ul style="list-style-type: none"> <li>Generally, de-identified information is personal information that has been modified so that an individual cannot be directly identified, though a risk of the individual being identified remains [2]</li> </ul>	<ul style="list-style-type: none"> <li>De-identified information is personal information that no longer allows the person concerned to be directly identified [12]</li> <li>When using de-identified information, reasonable steps</li> </ul>	<ul style="list-style-type: none"> <li>No specific provision</li> </ul>	<ul style="list-style-type: none"> <li>No specific provision</li> </ul>	<ul style="list-style-type: none"> <li>Pseudonymized information: <ul style="list-style-type: none"> <li>Personal data processed in such a manner that it can no longer be attributed to a specific individual without the use</li> </ul> </li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
		<ul style="list-style-type: none"> <li>De-identified information is still considered personal information (with exceptions) [2(3), see 22(1); 39(1), 55; 56; 63(1); 71-75; 116]</li> </ul>	shall be taken to limit the risk of anyone identifying a natural person based on this de-identified information [12]			of additional information kept separately, subject to technical and organizational measures [4(5)] ; consists of a security and privacy-by-design measure [25; 32]
<b>7. Sensitive information</b>	<ul style="list-style-type: none"> <li>No definition of “sensitive information”</li> <li>Recommendation to ensure a level of security appropriate to the sensitivity of the information [Sch. 1 – 4.7]</li> </ul>	<ul style="list-style-type: none"> <li>Personal information of minors is considered to be sensitive information [2(2)]</li> <li>Privacy management program must take into account sensitivity of the information [9(2); 62(1)]</li> <li>Retention periods must consider the sensitivity of personal information [9(1); 53(2)] and, where applicable, must be made readily available with respect to sensitive personal information [62(2)(e)]</li> <li>The sensitivity of the information must be taken into account in several other situations [see 12(2); 15(5); 22(b)(ii); 22(3)(a)(ii); 57(1); 58(8)(a); 74; 109(c)]</li> </ul>	<ul style="list-style-type: none"> <li>Information is considered “sensitive” if it entails a high level of reasonable expectation of privacy (including medical, biometric or otherwise intimate information) [12]</li> <li>Security measures must be appropriate with respect to the sensitivity of the information [10]</li> <li>Consent to the use or communication of sensitive personal information must be given expressly [12; 13]</li> <li>Sensitivity of the information must be taken into account in several other situations [see 3.3; 3.7; 17; 28.1; 90.2; 92.3]</li> </ul>	<ul style="list-style-type: none"> <li>No definition of “sensitive information”</li> <li>If implicit consent, then the collection, use or disclosure of personal information must be reasonable having regard to its sensitivity [8(3)]</li> </ul>	<ul style="list-style-type: none"> <li>No definition of “sensitive information”</li> <li>If implicit consent, then the collection, use or disclosure of personal information must be reasonable having regard to its sensitivity [8(3)]</li> </ul>	<ul style="list-style-type: none"> <li>Particular regime for “special categories of personal data” (including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation) [9]</li> <li>No separate regime for financial data</li> </ul>
<b>8. Consent</b>	<ul style="list-style-type: none"> <li>May be express or implied depending on the circumstances and the type of information, taking into account the reasonable expectations of the individual concerned [Sch. 1 – 4.3.5]</li> <li>Should generally be express when processing sensitive information [Sch. 1 – 4.3.6]</li> </ul>	<ul style="list-style-type: none"> <li>Must be obtained at or before the time of the collection [15(1)(2)]</li> <li>Must inform individuals, in plain language, of the type of personal information they collect, use, and disclose, and of the purposes, manner, consequences of such collection, use, and disclosure and the third parties to whom personal</li> </ul>	<ul style="list-style-type: none"> <li>Must be clear, free and informed and be given for specific purposes. It must be requested for each purpose, in clear and simple language [14]</li> <li>If request for consent is made in writing, it must be presented separately from any other</li> </ul>	<ul style="list-style-type: none"> <li>May be express or implied, each subject to specified requirements and limitations [8]</li> <li>May be withdrawn at any time on reasonable notice, unless withdrawing consent would frustrate</li> </ul>	<ul style="list-style-type: none"> <li>May be express or implied, each subject to specified requirements and limitations [7;8]</li> <li>May be withdrawn at any time on reasonable notice, unless withdrawing consent would frustrate</li> </ul>	<ul style="list-style-type: none"> <li>Must be freely given, specific, informed and unambiguous, in an intelligible and accessible form, and is only valid for specified purposes [4(11)]</li> <li>Must be “explicit” for the processing of special</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
	<ul style="list-style-type: none"> <li>• May be withdrawn at any time, subject to legal or contractual restrictions and reasonable notice [Sch. 1 – 4.3.8]</li> <li>• An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. [5(3)]</li> </ul>	<p>information will be disclosed [15(3)(4)]</p> <ul style="list-style-type: none"> <li>• Consent must be given expressly, except when it is “appropriate” to rely on implied consent, taking into account the reasonable expectations of the individual and the sensitivity of the personal information [15(5)-15 (6); 18]</li> <li>• May be withdrawn at any time, in whole or in part, subject to the CPPA, a federal or provincial law or to the reasonable terms of a contract [17]</li> <li>• An organization may collect, use or disclose personal information only in a manner and for purposes that a reasonable person would consider are appropriate in the circumstances, regardless of whether consent is required under the CPPA. [12(1)]</li> </ul>	<p>information provided to the person concerned [14]</p> <ul style="list-style-type: none"> <li>• Such consent is valid only for the length of time needed to achieve the purposes for which it was requested [14]</li> <li>• Consent not given in accordance with the Act is without effect [14]</li> <li>• Consent to the use or communication of sensitive personal information must be given expressly [12;13]</li> <li>• Consent to the communication or use of personal information may be withdrawn [8(4)]</li> <li>• when addressing a person for commercial or philanthropic prospection, such person must be informed of their right to withdraw consent to the use of their personal information for prospection purposes [22]</li> </ul>	<p>performance of a legal obligation [9]</p>	<p>performance of a legal obligation [9]</p>	<p>categories of personal data [9(2)(a)]</p> <ul style="list-style-type: none"> <li>• May be withdrawn at any time [7(3)]</li> </ul>
<b>9. Exceptions to consent</b>	<p><u>Collection, use and disclosure</u></p> <ul style="list-style-type: none"> <li>• Not required when exceptions apply (for example, in the case of a “prospective business transaction”) [7.2]</li> </ul>	<p><u>Collection, use and disclosure</u></p> <ul style="list-style-type: none"> <li>- Not required when exceptions apply, for example:</li> <li>- for the collection and use of personal information for certain business activities [15(6); 18]</li> <li>- for the collection and use of personal information for a legitimate interest, subject to multiple requirements, including the conduct of an assessment</li> </ul>	<p><u>Use</u></p> <ul style="list-style-type: none"> <li>• Not required when exceptions apply, for example when it is used for purposes consistent with the purposes for which it was collected [12]</li> </ul> <p><u>Communication</u></p> <ul style="list-style-type: none"> <li>• Not required when exceptions apply, for example when it is necessary to conclude a commercial transaction [18.4]</li> </ul>	<p><u>Collection, use and disclosure</u></p> <ul style="list-style-type: none"> <li>• Not required when exceptions apply (for example, in the case of a “business transaction”) [22]</li> </ul>	<p><u>Collection, use and disclosure</u></p> <ul style="list-style-type: none"> <li>• Not required when exceptions apply (for example, in the case of a “business transaction”) [20]</li> </ul>	<p><u>Processing</u></p> <ul style="list-style-type: none"> <li>• Another legal ground may apply, such as the necessity for the performance of a contract or the legitimate purposes of the controller [6(1)]</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
		<p>and record keeping obligations [18(3)(4)(5)]</p> <ul style="list-style-type: none"> <li>- for public interest [29-39]</li> <li>- to transfer personal information to service providers [2; 19]</li> <li>- for de-identified personal information in certain cases, notably in the context of a prospective business transaction [2; 20-22]</li> <li>- for the use and disclosure of personal information, in the context of a business transaction where de-identification would undermine the objectives of the transaction and the organization has taken into account the risk of harm to the individual that could result from using or disclosing the personal information [22(2)]</li> </ul>				
<b>10. Children</b>	<ul style="list-style-type: none"> <li>• No minimum age in PIPEDA for minor consent, but OPC <a href="#">Guidance for obtaining meaningful consent</a> states that the consent of a parent or guardian is generally required for children under the age of 13</li> </ul>	<ul style="list-style-type: none"> <li>• No minimum age in CPPA for minor consent</li> <li>• The personal information of minors is deemed sensitive personal information [2(2)]</li> <li>• Further limitations on the ability of organizations to refuse the disposal requests of minors [55(2)]</li> <li>• Parents are enabled to act on behalf of their children to protect their rights [4]</li> <li>• Minor is not defined in the CPPA.</li> </ul>	<ul style="list-style-type: none"> <li>• Consent to the collection of personal information concerning a minor under <u>14 years of age</u> must be given by the person having parental authority or the tutor, unless collecting the information is clearly for the minor's benefit [4.1; 14]</li> <li>• For minors aged <u>14 and over</u>, consent can also be given directly by the minor [14]</li> </ul>	<ul style="list-style-type: none"> <li>• No minimum age for the consent of minors, but must be old enough to provide meaningful consent</li> </ul>	<ul style="list-style-type: none"> <li>• No minimum age for the consent of minors, but must be old enough to provide meaningful consent</li> </ul>	<ul style="list-style-type: none"> <li>• Minimum age for minors consent is 16 years old [8(1)]</li> <li>• Member States may provide for a lower age than 16 years, provided that such lower age is not below 13 years [8(2)]</li> </ul>



## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
<b>11. Governance program</b>	<ul style="list-style-type: none"> <li>Organizations must have policies and practices with respect to the management of personal information [Sch. 1 – 4.8.1]</li> <li>Organizations must make readily available to individuals specific information about their policies and practices relating to the management of personal information [Sch. 1 - 4.8 see section on “<a href="#">Transparency</a>”]</li> </ul>	<ul style="list-style-type: none"> <li>Every organization must implement and maintain a privacy management program that includes the policies, practices and procedures the organization has put in place to fulfill its obligations under the CPPA, including policies, practices and procedures respecting: <ul style="list-style-type: none"> <li>the protection of personal information</li> <li>how requests for information and complaints are received and dealt with</li> <li>the training and information provided to the organization’s staff respecting its policies, practices and procedures and</li> <li>the development of materials to explain the organization’s policies and procedures [9; 62].</li> </ul> </li> <li>Organizations must make readily available, in plain language, information that explains the organization’s policies and practices [62(1), see section on “<a href="#">Transparency</a>”]</li> </ul>	<ul style="list-style-type: none"> <li>Every enterprise must establish and implement governance policies and practices regarding personal information that ensure the protection of such information [3.2]</li> <li>Such policies and practices must, in particular, provide a framework regarding: <ul style="list-style-type: none"> <li>the keeping and destruction of the information;</li> <li>the roles and responsibilities of the members of its personnel throughout the life cycle of the information and</li> <li>the process for dealing with complaints regarding the protection of the information [3.2].</li> </ul> </li> <li>Enterprises must publish detailed information about these policies, in clear and simple language, on its website [3.2]</li> </ul>	<ul style="list-style-type: none"> <li>Every organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under the PIPA AB [6(1)]</li> </ul>	<ul style="list-style-type: none"> <li>Every organization must: <ul style="list-style-type: none"> <li>develop and follow policies and practices that are necessary for the organization to meet the obligations under PIPA BC [5]</li> <li>develop a process to respond to complaints that may arise respecting the application of the PIPA BC [5].</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Controller shall implement appropriate data protection policies [24(2)]</li> <li>Data protection officer (see “privacy officer” section) shall monitor the policies of the controller in relation to the protection of personal data, including: <ul style="list-style-type: none"> <li>assignment of responsibilities;</li> <li>awareness-raising</li> <li>training of staff involved in the processing operations; and</li> <li>the related audits [39(1)].</li> </ul> </li> </ul>
<b>12. Rights of access</b>	<ul style="list-style-type: none"> <li>Yes, subject to certain exceptions to and prohibitions on disclosure. Exceptions include where information is subject to solicitor-client privilege or where the information contains references to third parties or cannot be disclosed for legal, security or commercial reasons [9; Sch.1-4.9]</li> </ul>	<ul style="list-style-type: none"> <li>Yes, subject to certain exceptions to and prohibition on disclosure. Exceptions include where giving access would reveal confidential commercial information, or doing so would threaten the life or security of another individual [70(7)]</li> </ul>	<ul style="list-style-type: none"> <li>Yes, subject to certain exceptions, including in cases of litigation or if it may seriously harm a third person [27; 37 and ss]</li> <li>Written request for access addressed to the person in charge of the protection of</li> </ul>	<ul style="list-style-type: none"> <li>Yes, subject to certain exceptions, including where the information is protected by legal privilege or disclosure could reveal personal information about or threaten the life or</li> </ul>	<ul style="list-style-type: none"> <li>Yes, subject to certain exceptions, including where the information is protected by solicitor-client privilege or disclosure could reveal personal information about or threaten the</li> </ul>	<ul style="list-style-type: none"> <li>Yes, subject to certain exceptions, including for legal or security reasons [15; 23]</li> <li>Where there are reasonable doubts concerning the identity of the individual concerned, it is possible to</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
<ul style="list-style-type: none"> <li>Request for access in writing [8(1)]</li> <li>Response within 30 days (this period may be extended by up to 30 days in certain cases) [8(3)]</li> <li>A charge may be required subject to certain conditions [8(6)]</li> <li>An organization shall assist any individual who requests assistance [8(2)]</li> </ul>	<ul style="list-style-type: none"> <li>Written request for access [64(1)]</li> <li>Response within 30 days (this period may be extended by up to 30 days in certain cases) [67]</li> <li>A charge may be required, subject to certain conditions [68]</li> <li>An organization shall assist any individual who requests assistance [64(2)]</li> </ul>	<p>personal information with proof of identity [30]</p> <ul style="list-style-type: none"> <li>Response in writing within 30 days, no possibility to extend the 30-day delay [32]</li> <li>The enterprise has an obligation to provide assistance [27; 29; 30]</li> <li>Free of charge (a reasonable charge may be required on certain conditions) [33]</li> <li>In case of refusal, the person in charge of the protection of personal information must give the reasons for such refusal and indicate the provisions of law on which the refusal is based, remedies that are available and specify the time limit for exercising them. Must also help to understand the refusal [34]</li> <li>Specific obligations for computerized personal information [27]<sup>7</sup></li> <li>The enterprise must inform the person of his right of access when his personal information is collected [8]</li> </ul>	<p>security of another individual [24]</p> <ul style="list-style-type: none"> <li>Request for access in writing</li> <li>Response within 45 calendar days (this period may be extended)</li> <li>A charge may be required subject to certain conditions</li> <li>An organization must make every reasonable effort to assist each applicant</li> </ul>	<p>health or safety of another individual [23]</p> <ul style="list-style-type: none"> <li>Request for access in writing</li> <li>Response within 30 business days (this period may be extended)</li> <li>A charge may be required subject to certain conditions</li> <li>An organization must make a reasonable effort to assist each applicant</li> </ul>	<p>request confirmation of his/her identity [12(6)]</p> <ul style="list-style-type: none"> <li>Response given in writing or orally (when requested by the individual concerned) [12(1)]</li> <li>Response shall be given without undue delay and in any event within one (1) month (this period may be extended) [12(3)]</li> <li>Free of charge (a reasonable charge may be required, subject to certain conditions) [12(5)]: <ul style="list-style-type: none"> <li>Obligation to facilitate the exercise of rights of access [12(2)].</li> </ul> </li> </ul>

7. The right to “data portability” will come into force on September 22, 2024.

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
<b>13. Right to correct (or to rectify)</b>	<ul style="list-style-type: none"> <li>Yes, if the information is inaccurate or incomplete [Sch. 1 – 4.9.5]</li> </ul>	<ul style="list-style-type: none"> <li>Yes, if the individual demonstrates that the information is not accurate, up-to-date or complete, the organization must amend the information [71(1)]</li> <li>The organization must, if it is appropriate to do so, transmit the amended information to any party that has access to the information [71(2)]</li> </ul>	<ul style="list-style-type: none"> <li>Yes, if the information is inaccurate, incomplete or equivocal, or if collecting, communicating or keeping it is not authorized by law [28]</li> <li>Rights of access requirements apply with the necessary changes</li> </ul>	<ul style="list-style-type: none"> <li>Yes, if there is an error or omission in the personal information [25]</li> <li>Request for correction in writing</li> <li>Must correct information as soon as reasonably possible</li> <li>No fee may be charged</li> </ul>	<ul style="list-style-type: none"> <li>Yes, if there is an error or omission in the personal information [24]</li> <li>Request for correction in writing</li> <li>Must correct information as soon as reasonably possible</li> <li>No fee may be charged</li> <li>If correction not agreed to, must annotate the record</li> </ul>	<ul style="list-style-type: none"> <li>Yes, if the data is inaccurate or incomplete [16]</li> <li>Rights of access requirements apply with the necessary changes</li> </ul>
<b>14. Right to erasure (or “right to be forgotten”)</b>	<ul style="list-style-type: none"> <li>No</li> </ul>	<ul style="list-style-type: none"> <li>A form of this right is contemplated by the CPPA, specifically to dispose of an individual’s personal information under the organization’s control (subject to certain conditions and exceptions) and to request that the organization inform any service provider to which it has transferred the information of the request and ensure that the service provider has disposed of the information [55]</li> <li>No express right to de-index or re-index a hyperlink at the individual’s request</li> </ul>	<ul style="list-style-type: none"> <li>Yes, to cease dissemination of the information, de-index or re-index any hyperlink attached to the name of the person concerned that provides access to the information by a technological means [28.1]</li> <li>Only if the dissemination contravenes the law or if certain conditions are met [28.1]</li> <li>Written request for access addressed to the person in charge of the protection of personal information with proof of identity [30]</li> <li>Response in writing within 30 days [32]</li> <li>The enterprise has an obligation to provide assistance [30]</li> </ul>	<ul style="list-style-type: none"> <li>No</li> </ul>	<ul style="list-style-type: none"> <li>No</li> </ul>	<ul style="list-style-type: none"> <li>Yes (subject to certain conditions) [17]</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
			<ul style="list-style-type: none"> <li>In case of refusal, the person in charge of the protection of personal information must give the reasons for any refusal and indicate the provision of law on which the refusal is based, remedies available and specify the time limit for exercising them. Must also help to understand the refusal [34]</li> </ul>			
<b>15. Other rights of individuals</b>	<ul style="list-style-type: none"> <li>Right to address a challenge concerning non-compliance with PIPEDA to the organization [Sch. 1 – 4.10]</li> <li>Right to file a complaint with the OPC [11(1)]</li> </ul>	<ul style="list-style-type: none"> <li>Right to file a complaint with the organization [73]</li> <li>Right to file a complaint with the OPC [82]</li> <li>Right to be informed if an automated decision system made a prediction, decision or recommendation that has a significant impact on the individual [63(3)]</li> <li>Right to personal data portability where both organizations are subject to a “data mobility framework” [72;123]</li> </ul>	<ul style="list-style-type: none"> <li>Right to file a complaint with the enterprise [3.2]</li> <li>Right to file a complaint with the CAI [81]</li> <li>Right to submit an application to the CAI for the examination of a disagreement [42]</li> <li>Right to be informed if a decision based exclusively on an automated processing of personal information is made to, notably, submit observations and ask for a revision of such decision [12.1]</li> <li>Right to obtain personal information in a structured, commonly used format, and to have the information communicate, at the applicant’s request, to any person or body authorized by law to collect such information [27]</li> </ul>	<ul style="list-style-type: none"> <li>Right to file a complaint with the OIPC AB or to request a review of a decision by an organization regarding an individual’s request respecting personal information [36]</li> </ul>	<ul style="list-style-type: none"> <li>Right to make a complaint to the organization [46]</li> <li>Right to file a complaint with the OIPC BC or to request a review of a decision by an organization regarding an individual’s request to access or correct personal information [47]</li> </ul>	<ul style="list-style-type: none"> <li>Right to lodge a complaint with the competent supervisory authority [77]</li> <li>Right to restriction of processing of personal data [18]</li> <li>Right to personal data portability [20]</li> <li>Right to object to processing of personal data [21]</li> <li>Right not to be subject to a decision based solely on automated processing [22]</li> </ul>
<b>16. Privacy Officer</b>	<ul style="list-style-type: none"> <li>Obligation to designate an individual who is accountable for compliance</li> </ul>	<ul style="list-style-type: none"> <li>Obligation to designate one or more individuals to be responsible</li> </ul>	<ul style="list-style-type: none"> <li>The person with the highest authority is responsible to</li> </ul>	<ul style="list-style-type: none"> <li>Organization must designate one or more individuals to be</li> </ul>	<ul style="list-style-type: none"> <li>Organization must designate one or more individuals to be</li> </ul>	<ul style="list-style-type: none"> <li>Obligation to designate a “data protection officer” in certain circumstances,</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
	with PIPEDA and to disclose such individual's identity [Sch. 1 – 4.1]	for the organization's compliance with CPPA [8(1)] <ul style="list-style-type: none"> <li>The designated individual(s) business contact information must be provided to anyone who requests it [8(1)]</li> <li>The designated individual(s) is(are) not necessarily the one(s) to whom complaints and requests under the CPPA are made [62(2)(g) read with 8(1)]</li> </ul>	ensure the Act is implemented and complied with [3.1] <ul style="list-style-type: none"> <li>This function may be delegated, in writing, to any person [3.1]</li> <li>This person must approve the policies and practices of the enterprise [3.2]</li> <li>This person must be consulted for any assessment of the privacy-related factors [3.3]</li> <li>This person may suggest any personal information protection measures applicable to a project of acquisition, development or redesign of an information system [3.4]</li> <li>This person must be consulted in assessing the risk of injury to a person whose personal information is concerned by a confidentiality incident [3.7]</li> <li>This person is in charge of the access, rectification or "erasure" requests [28.1; 30; 32; 34; 35]</li> </ul>	responsible for compliance with PIPA AB [5(3)]	responsible for compliance with PIPA BC, and must make available the position name or title and contact information for each such individual [4(3)]	including the processing on a large scale of special categories of data or the processing operations that require regular and systematic monitoring of the individuals concerned on a large scale [37]
<b>17. Transparency</b>	<ul style="list-style-type: none"> <li>Organizations must make readily available to individuals, in a form that is generally understandable, the policies and practices relating to the management of personal information [Sch. 1 – 4.8]</li> </ul>	<ul style="list-style-type: none"> <li>Organizations must make readily available, in plain language, information that explain their policies and practices [9; 62(1)], including:</li> </ul>	<ul style="list-style-type: none"> <li>Enterprises must publish detailed information about their policies and practices in simple and clear language [3.2]</li> <li>If personal information is collected through technological means, the enterprise must</li> </ul>	<ul style="list-style-type: none"> <li>Organizations must make information available on request about its policies and practices for compliance with PIPA AB, including</li> </ul>	<ul style="list-style-type: none"> <li>Organizations must make information available on request about its policies and practices for compliance with PIPA BC, and about its process for</li> </ul>	<ul style="list-style-type: none"> <li>Organizations must provide to the individual concerned a wide variety of information at the time when the data are obtained (purposes of the processing, legal grounds, recipients, transfer</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
<ul style="list-style-type: none"> <li>Organizations must inform the individual of the type of personal information held by the organization, including a general account of its use, with any additional details [Sch. 1 – 4.8]</li> <li>Organizations must be able to explain to individuals the purposes for which the information is being collected [Sch. 1 – 4.8]</li> </ul>	<ul style="list-style-type: none"> <li>a description of the type of personal information under its control</li> <li>a general account of how the organization uses the personal information and of how it applies consent exceptions</li> <li>a general account of its use of automated decision-making that could have a significant impact on them</li> <li>whether it carries out interprovincial or international transfers or disclosures that may have reasonably foreseeable privacy implications</li> <li>retention periods applicable to sensitive information</li> <li>disposal and access rights or</li> <li>the contact information of the individual to whom complaints or requests for information may be made [62(2)].</li> <li>To obtain a valid consent, organizations must inform individuals in plain language, before or at the time of the collection, of:             <ul style="list-style-type: none"> <li>the purposes for the collection, use or disclosure of personal information</li> <li>the manner in which personal information is to be collected, used or disclosed</li> <li>any reasonably foreseeable consequences of the collection,</li> </ul> </li> </ul>	<p>publish a confidentiality policy in clear and simple language on its website [8.2]</p> <ul style="list-style-type: none"> <li>To obtain valid consent [8.3], enterprises must inform individuals, before or when collecting personal information, of:             <ul style="list-style-type: none"> <li>the purposes for which the information is collected</li> <li>the means by which it is collected</li> <li>their rights to access and rectification</li> <li>their right to withdraw consent</li> <li>the name of the third person for whom the information is being collected (if any)</li> <li>the names of the third persons or the categories of third persons to whom communication is necessary</li> <li>the possibility that the information may be communicated outside Québec [8] and</li> <li>the use of a technology that includes functions of identification, location or profiling and inform him of the means available to activate those functions [8.1].</li> </ul> </li> <li>No later than at the time a person is informed of a decision made exclusively with automated decision-making,</li> </ul>	<p>information about its use of services providers outside Canada to collect, use, disclose or store personal information [6]</p>	<p>responding to complaints [5]</p>	<p>of data, period of storage, applicable rights, contact details of the controller or the data protection officer, etc.) [13]</p> <ul style="list-style-type: none"> <li>Where personal data have not been obtained from the data subject, information including the identity of the controller, the recipients of the personal data, etc. [14]</li> <li>Provide any information in a concise, transparent, intelligible and easily accessible form, using clear and plain language [12(1)]</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
		<p>use and disclosure of personal information</p> <ul style="list-style-type: none"> <li>- the specific type of personal information that is collected, used or disclosed; and</li> <li>- the names of third parties or types of third parties to which the organization may disclose personal information [15(3)].</li> </ul>	<p>enterprises must inform individuals about the use of such technology accordingly [12.1]</p> <ul style="list-style-type: none"> <li>• Enterprises must publish the title and contact information of the privacy officer on its website or, if the enterprise does not have a website, be made available by any other appropriate means [3.1]</li> <li>• Enterprises must inform the public of the place where, and manner in which, access to personal information may be granted [29]</li> <li>• When personal information is used for commercial or philanthropic prospection purposes, the person must identify himself and inform the person concerned of their right to withdraw their consent to the use of their personal information for such purposes [22]</li> </ul>			
<b>18. Security measures</b>	<ul style="list-style-type: none"> <li>• Organizations must implement security measures, including physical, organizational and technological measures, depending on the sensitivity of the information, the amount, distribution, and format of the information, and the method of storage [Sch. 1 – 4.7]</li> <li>• Obligation to make employees aware of the importance of</li> </ul>	<ul style="list-style-type: none"> <li>• Organizations must protect personal information through physical, organizational and technological security safeguards. The level of protection provided by those safeguards must be proportionate to the sensitivity of the information [57]</li> </ul>	<ul style="list-style-type: none"> <li>• Enterprises must implement security measures necessary to ensure the protection of the personal information that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored [10]</li> </ul>	<ul style="list-style-type: none"> <li>• Organizations must make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction [34]</li> </ul>	<ul style="list-style-type: none"> <li>• Organizations must make reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks [34]</li> </ul>	<ul style="list-style-type: none"> <li>• Organizations must implement technical and organizational measures to ensure a level of security appropriate to the risk (including pseudonymisation and encryption of data, as appropriate) [32]</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
	maintaining the confidentiality of personal information [Sch. 1 – 4.7.4]					
<b>19. Breach definition</b>	<ul style="list-style-type: none"> <li>A breach of security safeguards means the loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization’s security safeguards [2(1)]</li> </ul>	<ul style="list-style-type: none"> <li>A breach of security safeguards means the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization’s security safeguards [2(1)]</li> </ul>	<ul style="list-style-type: none"> <li>A confidentiality incident means:               <ul style="list-style-type: none"> <li>- access not authorized by law to personal information</li> <li>- use not authorized by law of personal information</li> <li>- communication not authorized by law of personal information</li> <li>- loss of personal information or</li> <li>- any other breach of the protection of such information [3.6].</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>An incident means one that involves the loss of or unauthorized access to or disclosure of the personal information [34.1]</li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>	<ul style="list-style-type: none"> <li>A personal data breach means a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed [4(12)]</li> </ul>
<b>20. Breach notification</b>	<ul style="list-style-type: none"> <li>Mandatory notification to the OPC, as soon as feasible, of any breach that creates a “real risk of significant harm” [10.1]</li> <li>Mandatory notification to individuals, as soon as feasible, of any breach that creates a “real risk of significant harm” [10.1(3)]</li> <li>Mandatory notification to any other organization, government institution or part of a government institution that could reduce the risk [10.2]</li> <li>Keep a record of every data breach and, on request, provide the OPC with access to the record [10.3]</li> </ul>	<ul style="list-style-type: none"> <li>Mandatory notification to the OPC as soon as feasible of any breach that creates a “real risk of significant harm” [58]</li> <li>Mandatory notification to individuals, as soon as feasible, of any breach that creates a “real risk of significant harm” for them [58]</li> <li>Mandatory notification to any other organization, government institution or part of a government institution that could reduce the risk [59]</li> <li>Requirement to keep and maintain a record of every breach and, on request, provide the OPC with access to the record [60]</li> </ul>	<ul style="list-style-type: none"> <li>Mandatory notification to the CAI of any incident that presents a risk of serious injury [3.5]</li> <li>Mandatory notification to any person whose personal information is concerned by the confidentiality incident that presents a risk of serious injury, unless doing so could hamper an investigation [3.5]</li> <li>Optional notification to any person or body that could reduce the risk [3.5]</li> <li>Requirement to keep and maintain a register of confidentiality incidents for five years after the incident, and on</li> </ul>	<ul style="list-style-type: none"> <li>Mandatory notification to the OIPC AB as soon as feasible of any unauthorized access to or disclosure of personal information that creates a “real risk of significant harm” [34.1]</li> <li>OIPC AB may require notification to individuals for whom there is a “real risk of significant harm” [Personal Information Protection Act Regulation]</li> </ul>	<ul style="list-style-type: none"> <li>No requirement</li> <li>Optional notification to OIPC BC</li> </ul>	<ul style="list-style-type: none"> <li>Mandatory notification to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of the incident in certain circumstances [33]</li> <li>Communicate with the individual concerned without undue delay where the data breach is likely to result in a high risk to rights and freedoms, subject to certain conditions [33]</li> </ul>



## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
		<ul style="list-style-type: none"> <li>Service providers must notify every breach to the organization that controls the personal information [61]</li> </ul>	<p>request, provide the CAI with access to the register [3.8]</p> <ul style="list-style-type: none"> <li>A regulation determines the content and terms of the notices and of the register of confidentiality incidents [3.5; 3.8]</li> <li>If an enterprise believes that a confidentiality incident occurred, it must take reasonable measures to reduce the risk of injury and prevent new incidents of the same nature [3.5]</li> </ul>			
<b>21. Transfer to foreign jurisdictions permitted</b>	<ul style="list-style-type: none"> <li>Outside Canada</li> <li>Yes, by way of contract or otherwise, provided that a comparable level of protection is provided for the personal information [4.1.3]</li> <li>The individuals must be informed that their information may be sent to a foreign country for processing purposes and that it may be accessible to the courts and the law enforcement and national security authorities of that jurisdiction [according to the <a href="#">Processing Personal Data Across Borders Guidelines</a>]</li> <li>Under specific conditions, the OPC may disclose information to any</li> </ul>	<ul style="list-style-type: none"> <li>Outside Canada</li> <li>Yes, as long as the organization informs the individuals that they carry out an international or interprovincial transfer of personal information that may have reasonably foreseeable privacy implications [62(2)(d)]</li> <li>To a “service provider” [2], without knowledge or consent of the individual, if the organization ensures, by contract or otherwise, that the service provider provides a level of protection of the personal information equivalent to that which the organization is required to provide under the CPPA [7; 11]</li> </ul>	<ul style="list-style-type: none"> <li>Outside Québec</li> <li>Yes, after the conduction of a privacy impact assessment (“PIA”), taking into account: <ul style="list-style-type: none"> <li>the sensitivity of the information;</li> <li>the purposes for which it is to be used</li> <li>the protection measures, including contractual ones, that would apply and</li> <li>the legal framework applicable in the State in which the information would be communicated, in particular the data protection principles applicable in the foreign State [17].</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Outside Alberta</li> <li>Yes, but if organization uses a service provider outside Canada to collect, use, disclose or store personal information, then the privacy policy must disclose information regarding: <ul style="list-style-type: none"> <li>the countries outside Canada in which the collection, use, disclosure or storage may occur and</li> <li>the purposes for which the service provider outside Canada has been authorized to collect,</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Outside British Columbia</li> <li>Yes, but disclosure in privacy policy recommended by OIPC BC</li> </ul>	<ul style="list-style-type: none"> <li>Outside the EU/EEA</li> <li>Yes, if there is an “adequacy decision” or other appropriate safeguards under the GDPR, such as standard contractual clauses approved by the European Commission, binding corporate rules, adherence to a code of conduct or certification mechanism [44 to 47]</li> <li>Prior to the appropriate safeguards, transfer risk assessments [Schrems II]</li> <li>Obligation to designate a “representative” in an extraterritorial context, if no establishment in the EU,</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
	person or body under the legislation of a foreign state [23.1]	<ul style="list-style-type: none"> <li>The OPC may disclose information to a foreign state under specific conditions [120]</li> </ul>	<ul style="list-style-type: none"> <li>The information may be communicated if the assessment allows to conclude that the information would receive an adequate protection under generally accepted privacy principles [17]</li> <li>- The communication must be the subject of a written agreement [17]</li> </ul>	use or disclose personal information [6(2)].		<p>but targeting the EU market [27]</p> <ul style="list-style-type: none"> <li>Some derogations to the requirements for adequacy decision and appropriate safeguards for specific situations [49]</li> </ul>
<b>22. Privacy by design</b>	<ul style="list-style-type: none"> <li>No express requirement. However, an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. [5(3)]</li> <li>Collection, use and disclosure of personal information shall be limited to that which is necessary for the purposes identified by the organization [Schedule 1, 4.4, 4.5]</li> </ul>	<ul style="list-style-type: none"> <li>No express requirement. However, an organization may collect, use or disclose personal information only in a manner and for purposes that a reasonable person would consider are appropriate in the circumstances, regardless of whether consent is required under the CPPA. [12(1)]</li> <li>An organization may only collect personal information that is necessary for the purposes that the organization has determined and recorded prior to collection, and must not use or disclose personal information except for those purposes, with the further valid consent of the individual, or in the circumstances set out in the CPPA [13; 14]</li> </ul>	<ul style="list-style-type: none"> <li>If the enterprise offers technological products or services to the public that have privacy parameters, those parameters must, by default, provide the highest level of confidentiality (except for the privacy settings of cookies) [9.1]</li> </ul>	<ul style="list-style-type: none"> <li>No express requirement. However, an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. [2, 3]</li> </ul>	<ul style="list-style-type: none"> <li>No express requirement. However, an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. [2]</li> </ul>	<ul style="list-style-type: none"> <li>The controller must implement appropriate technical and organizational measures, such as pseudonymisation, designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects [25(1)]</li> </ul>
<b>23. New projects involving personal information</b>	<ul style="list-style-type: none"> <li>No specific requirement for a PIA</li> <li><a href="#">Recommended by the OPC</a></li> </ul>	<ul style="list-style-type: none"> <li>No specific requirement for a PIA</li> <li><a href="#">Recommended by the OPC</a></li> </ul>	<ul style="list-style-type: none"> <li>Enterprises must conduct a PIA for any project of acquisition, development and redesign of an information system [3.3]</li> </ul>	<ul style="list-style-type: none"> <li>No specific requirement for a PIA</li> <li><a href="#">Recommended by the OIPC AB</a></li> </ul>	<ul style="list-style-type: none"> <li>No specific requirement for a PIA</li> <li><a href="#">Recommended by the OIPC BC</a></li> </ul>	<ul style="list-style-type: none"> <li>Data-protection impact assessment required in certain circumstances [35]</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
<b>24. Audits</b>	<ul style="list-style-type: none"> <li>The OPC may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if it 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 [18-19]</li> </ul>	<ul style="list-style-type: none"> <li>The OPC may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if it has reasonable grounds to believe that the organization has contravened, is contravening or is likely to contravene the CPPA's part 1 (obligations of organizations) [97-99]</li> </ul>	<ul style="list-style-type: none"> <li>The CAI may, by a formal demand notified by any appropriate method, require any person to file, within a time specified in the demand, any information or document to verify compliance with the law [81.3]</li> <li>This applies to enterprises as well [83.1]</li> </ul>	<ul style="list-style-type: none"> <li>The OIPC AB may conduct an investigation to ensure compliance with any provision of PIPA AB [36(1)(a)]</li> </ul>	<ul style="list-style-type: none"> <li>The OIPC BC may, whether a complaint is received or not, initiate investigations and audits to ensure compliance with any provisions of PIPA BC, if the commissioner is satisfied there are reasonable grounds to believe that an organization is not complying with PIPA BC [36(1)(a); 38; 41(2)(3)]</li> </ul>	<ul style="list-style-type: none"> <li>Each supervisory authority may, in the form of data protection audits, carry out investigations [58]</li> </ul>
<b>25. Retention of information</b>	<ul style="list-style-type: none"> <li>For such time as is necessary for the purposes identified or to allow the individual to exhaust any recourse provided by law [8(8)]</li> <li>Maintain personal information as accurate, complete, and up to date as is necessary for the purposes for which it is to be used [Sch. 1 – 4.6]</li> </ul>	<ul style="list-style-type: none"> <li>For a period no longer than necessary to fulfill the purposes for which the information was collected, used or disclosed or to comply with applicable laws [53(1)]</li> <li>When determining the retention period, the organizations must take into account the sensitivity of the information [53(2)]</li> <li>When making a decision about an individual, the organization must retain the personal information used to make the decision for a sufficient period of time to allow the individual to make a request for access [54;63;69]</li> <li>As long as necessary to exhaust any recourse an individual has under the CPPA [63;69]</li> <li>At the individual's request, the organization must dispose of their</li> </ul>	<ul style="list-style-type: none"> <li>For such time as is necessary for the purposes identified to be achieved [23]</li> <li>If a request of access or rectification is denied: for such time as is necessary to allow the person concerned to exhaust the recourses provided by law [36]</li> <li>Ensure that any personal information held on another individual is up to date and accurate when used by an enterprise to make a decision in relation to the individual concerned. Following that decision, the information used is kept for at least one year [11]</li> <li>Organizations must provide a framework for the keeping and destruction of the information in</li> </ul>	<ul style="list-style-type: none"> <li>For only as long as the organization reasonably requires the personal information for legal or business purposes [35(1)]</li> <li>The organization must then (a) destroy the records containing the personal information, or (b) render the personal information non-identifying so that it can no longer be used to identify an individual [35(2)]</li> </ul>	<ul style="list-style-type: none"> <li>Must destroy its records containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that (a) the purpose is no longer being served by retention of the personal information, and (b) retention is no longer necessary for legal or business purposes [35]</li> <li>If an organization uses an individual's personal information to make a decision that directly affects the individual, the organization must retain</li> </ul>	<ul style="list-style-type: none"> <li>For such time as is necessary but limited to a strict minimum [r. 39]</li> <li>Records of processing activities required, except for an organization employing fewer than 250 persons, subject to certain conditions [30]</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
		<p>personal information (with exceptions) [55]</p> <ul style="list-style-type: none"> <li>Maintain personal information as accurate, up-to-date and complete as is necessary for the purposes [56]</li> </ul>	its governance policies and practices [3.2]		that information for at least one year [35]	
<b>26. Statutory penalties</b>	<p><u>Monetary penalties</u></p> <ul style="list-style-type: none"> <li>N/A</li> </ul>	<p><u>Monetary penalties</u></p> <ul style="list-style-type: none"> <li>Upon the OPC's recommendations, the Tribunal may impose a penalty up to: <ul style="list-style-type: none"> <li><b>\$10 million or 3%</b> of the organization's annual gross global revenue, whichever is greater [95].</li> </ul> </li> </ul>	<p><u>Monetary administrative penalties</u></p> <ul style="list-style-type: none"> <li>A person appointed by the CAI may impose administrative penalties for a contravention of the provisions of the law [as described at 90.1] up to: <ul style="list-style-type: none"> <li><b>\$50,000</b>, if the contravener is an individual</li> <li><b>\$10 million or 2%</b> of worldwide turnover for the preceding fiscal year, whichever is greater, in all other cases [90.12].</li> </ul> </li> <li>Possibility to avoid a penalty if the enterprise enters into an undertaking with the CAI [90.1]</li> <li>The amount of the penalty is determined according to different factors [90.2]</li> <li>No administrative penalty may be imposed on a person if a statement of offence has already been served on the person for the same reasons [90.11]</li> </ul>	<p><u>Monetary penalties</u></p> <ul style="list-style-type: none"> <li>N/A</li> </ul>	<p><u>Monetary penalties</u></p> <ul style="list-style-type: none"> <li>N/A</li> </ul>	<p><u>Monetary administrative fines</u></p> <ul style="list-style-type: none"> <li>A supervisory authority may impose administrative fines of, depending on the nature of the offence: <ul style="list-style-type: none"> <li>up to €10 million or 2% of the worldwide annual turnover; or</li> <li>up to <b>€20 million or 4%</b> of the worldwide annual turnover (whichever is higher) [83].</li> </ul> </li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
	<p><u>Penal provisions</u></p> <ul style="list-style-type: none"> <li>Where an organization knowingly contravenes provisions listed in section 28, it is liable to a fine: <ul style="list-style-type: none"> <li>up to <b>\$100,000</b> on indictment; or</li> <li>up to <b>\$10,000</b> (summary conviction) [28].</li> </ul> </li> </ul>	<p><u>Penal provisions</u></p> <ul style="list-style-type: none"> <li>Where an organization knowingly contravenes provisions listed in section 128 it is liable to a fine: <ul style="list-style-type: none"> <li>up to <b>\$25 million or 5%</b> of its annual gross global revenue, whichever is greater (on indictment); or</li> <li>up to <b>\$20 million or 4%</b> of its annual gross global revenues, whichever is greater (on summary conviction) [128].</li> </ul> </li> </ul>	<p><u>Penal provisions</u></p> <ul style="list-style-type: none"> <li>Anyone who contravenes section 91 is liable to a fine: <ul style="list-style-type: none"> <li>up to <b>\$100,000</b>, if the offender is an individual or</li> <li>up to <b>\$25 million or 4%</b> of their worldwide turnover for the preceding fiscal year, whichever is greater, in all other cases [91].</li> </ul> </li> <li>Fines for subsequent offences are doubled [92.1]</li> <li>The sentence is determined according to different factors [92.3]</li> </ul>	<p><u>Penal provisions</u></p> <ul style="list-style-type: none"> <li>Anyone who contravenes section 56 is liable to a fine: <ul style="list-style-type: none"> <li>up to <b>\$10,000</b> for individuals; and</li> <li>up to <b>\$100,000</b> for persons other than individuals [59(2)].</li> </ul> </li> </ul>	<p><u>Penal provisions</u></p> <ul style="list-style-type: none"> <li>Anyone who contravenes section 59 is liable to a fine: <ul style="list-style-type: none"> <li>up to <b>\$10,000</b> for individuals; and</li> <li>up to <b>\$100,000</b> for persons other than individuals [56].</li> </ul> </li> </ul>	<p><u>Penal provisions</u></p> <ul style="list-style-type: none"> <li>Member States shall lay down the rules on other penalties applicable to infringements of this GDPR in particular for infringements which are not subject to administrative fines [84]</li> </ul>
<b>27. Remedies from regulatory authority</b>	<ul style="list-style-type: none"> <li>Remedies available from the OPC [12]</li> </ul>	<ul style="list-style-type: none"> <li>Remedies available from the OPC [82]</li> <li>Orders by the OPC [93]</li> <li>Remedies available from the courts [including 104;105;106]</li> </ul>	<ul style="list-style-type: none"> <li>Remedies available from the CAI [81]</li> <li>Orders by the CAI [83]</li> </ul>	<ul style="list-style-type: none"> <li>Orders by the OIPC AB on the completion of an inquiry [52]</li> </ul>	<ul style="list-style-type: none"> <li>Orders by the OIPC BC on the completion of an inquiry [52]</li> </ul>	<ul style="list-style-type: none"> <li>Remedies available from the competent supervisory authority [77]</li> </ul>
<b>28. Private right of action</b>	<ul style="list-style-type: none"> <li>After receiving the OPC's investigation report or notification that its investigation has been completed or discontinued, a complainant may apply to court to seek damages (potentially by way of a class action) [14-16]</li> </ul>	<ul style="list-style-type: none"> <li>Where the Commissioner or Tribunal has found that an organization has contravened the CPPA, an individual has a cause of action against the organization in damages for loss or injury [107]</li> </ul>	<ul style="list-style-type: none"> <li>An individual may apply directly to a civil court to seek damages for loss or injury resulting from a breach of the law (including by way of a class action) [<i>Civil Code of Québec</i>]</li> <li>Where the infringement is intentional or results from gross negligence, the court awards punitive damages of not less than \$1,000 [93.1]</li> </ul>	<ul style="list-style-type: none"> <li>Where the OIPC AB has made a final order, an individual may apply to a court to seek damages for loss or injury resulting from a breach of PIPA AB [60]</li> </ul>	<ul style="list-style-type: none"> <li>Where the OIPC BC has made a final order, an individual may seek damages for actual harm resulting from a breach of PIPA BC [57]</li> </ul>	<ul style="list-style-type: none"> <li>Any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered (including by way of a collective action) [82]</li> </ul>

## Comparative Table of Personal Information Protection Laws (Canada)

	<i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i> <sup>1</sup>	<i>Consumer Privacy Protection Act (CPPA)</i> , as proposed in Bill C-27 <sup>2</sup>	<i>Act respecting the protection of personal information in the private sector</i> , as amended by Bill 64 <sup>3</sup>	<i>Alberta Personal Information Protection Act (PIPA AB)</i>	<i>BC Personal Information Protection Act (PIPA BC)</i>	<i>General Data Protection Regulation (GDPR)</i>
<b>29. Statutory certification programs</b>	<ul style="list-style-type: none"> <li>N/A</li> </ul>	<ul style="list-style-type: none"> <li>While it remains subject to its obligations under the CPPA [80], an organization may seek the approval of the OPC for a:               <ul style="list-style-type: none"> <li>- <u>Code of practice</u>: provides for substantially the same or greater protection of personal information as some or all of the protection provided under the CPPA [76] and</li> <li>- <u>Certification program</u>: a program that meets the criteria set out in the regulations (to come) [77].</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>	<ul style="list-style-type: none"> <li>Code of conduct or certification mechanism to facilitate monitoring of privacy compliance [40 to 43]</li> </ul>