



Tableau comparatif des lois pour la protection des renseignements personnels

AOÛT 2022

FASKEN

Table des matières

1.	Date d'entrée en vigueur	3	25.	Conservation des renseignements.....	22
2.	Autorité responsable.....	4	26.	Sanctions prévues par la loi	23
3.	Champ d'application	4	27.	Recours auprès de l'organisme de réglementation.....	25
4.	Renseignements personnels (ou « données à caractère personnel »).....	5	28.	Droit d'action privé	25
5.	Renseignements anonymisés.....	5	29.	Programmes légaux de certification	26
6.	Renseignements dépersonnalisés.....	6			
7.	Renseignements de nature sensible	7			
8.	Consentement	7			
9.	Exceptions applicables au consentement.....	9			
10.	Enfants	10			
11.	Programme de gouvernance	10			
12.	Droit d'accès.....	11			
13.	Droit de corriger (ou de rectifier).....	12			
14.	Droit à l'effacement (ou « droit à l'oubli »)	13			
15.	Autres droits des particuliers	14			
16.	Responsable de la protection de la vie privée	15			
17.	Transparence	16			
18.	Mesures de sécurité	18			
19.	Définition d'« atteinte aux mesures de sécurité »	19			
20.	Signalement d'une atteinte	19			
21.	Transfert permis vers des territoires étrangers.....	20			
22.	Confidentialité dès la conception	21			
23.	Nouveaux projets liés aux renseignements personnels.....	22			
24.	Vérifications	22			

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	 Canada	 Québec	 Alberta	 Colombie-Britannique	 Union européenne	
	<i>Loi sur la protection des renseignements personnels et les documents électroniques</i> (LPRPDE) ¹	<i>Loi sur la protection de la vie privée des consommateurs</i> (LPVPC), telle que proposée dans le projet de loi C-27 ²	<i>Loi sur la protection des renseignements personnels dans le secteur privé</i> , telle qu'amendée par le projet de loi 64 ³	<i>Personal Information Protection Act de l'Alberta</i> (PIPA de l'Alberta)	<i>Personal Information Protection Act de la Colombie-Britannique</i> (PIPA de la C.-B.)	<i>Règlement général sur la protection des données</i> (RGPD)
1. Date d'entrée en vigueur	<ul style="list-style-type: none"> 1^{er} janvier 2001, au Canada (s'applique à toutes les organisations depuis le 1^{er} janvier 2004) 	<ul style="list-style-type: none"> Pas en vigueur Présentée par le ministre de l'Innovation, des Sciences et de l'Industrie à la Chambre des communes le 16 juin 2022 	<ul style="list-style-type: none"> 22 septembre 2022 : en particulier, les exigences relatives à la désignation d'un responsable de la protection des renseignements personnels, le signalement obligatoire des incidents et la communication autorisée dans le cadre de transactions commerciales [liste exhaustive des articles entrant en vigueur : 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]⁴ 22 septembre 2023 : la majorité des dispositions 22 septembre 2024 : une forme de droit à la « portabilité » des données 	<ul style="list-style-type: none"> 1^{er} janvier 2004 	<ul style="list-style-type: none"> 1^{er} janvier 2004 	<ul style="list-style-type: none"> 25 mai 2018

1. Le 17 novembre 2020, le gouvernement canadien a déposé le [projet de loi C-11, la Loi de 2020 sur la mise en œuvre de la Charte du numérique](#) (C-11), qui apporte des changements substantiels à la législation canadienne relative à la protection des renseignements personnels. Le projet de loi C-11 proposait (i) d'édicter la *Loi sur la protection de la vie privée des consommateurs* pour remplacer la partie 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui concerne la protection des renseignements personnels dans le secteur privé, et (ii) d'édicter la *Loi sur le Tribunal de la protection des renseignements personnels et des données*, qui institue le Tribunal de la protection des renseignements personnels et des données, lequel serait saisi des recommandations et des appels des décisions du commissaire à la protection de la vie privée du Canada (le commissaire). Cependant, la dissolution du gouvernement a mis fin à tous les travaux en cours au Sénat et à la Chambre des communes, y compris le projet de loi C-11.

2. Le 16 juin 2022, le gouvernement canadien a déposé le [projet de loi C-27, la Loi de 2022 sur la mise en œuvre de la Charte du numérique](#), qui apporte des changements substantiels à la législation canadienne relative à la protection des renseignements personnels. En plus d'édicter la LPVPC et la *Loi sur l'intelligence artificielle et les données* (versions proposées lors des derniers efforts du gouvernement fédéral pour réformer la protection des renseignements personnels en novembre 2020), le projet de loi C-27 propose d'adopter la *Loi sur l'intelligence artificielle et les données* (LIAD) pour réglementer les « systèmes d'intelligence artificielle » et le traitement des données liées aux systèmes d'intelligence artificielle.

3. Les références faites à cette loi dans la présente colonne sont des références à la Loi telle que modifiée par le projet de loi 64 (aussi appelé « Loi 25 »). Pour connaître les dates d'entrée en vigueur des modifications, consultez [notre version annotée de la Loi, telle que modifiée par le projet de loi 64](#).

4. Les chiffres entre crochets renvoient au numéro d'article de la loi mentionnée.

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques</i> (LPRPDE) ¹	<i>Loi sur la protection de la vie privée des consommateurs</i> (LPVPC), telle que proposée dans le projet de loi C-27 ²	<i>Loi sur la protection des renseignements personnels dans le secteur privé</i> , telle qu'amendée par le projet de loi 64 ³	<i>Personal Information Protection Act</i> de l'Alberta (PIPA de l'Alberta)	<i>Personal Information Protection Act</i> de la Colombie-Britannique (PIPA de la C.-B.)	<i>Règlement général sur la protection des données</i> (RGPD)
2. Autorité responsable	<ul style="list-style-type: none"> Commissariat à la protection de la vie privée du Canada (CPVP) [2; 11] 	<ul style="list-style-type: none"> Commissariat à la protection de la vie privée du Canada (CPVP) [2; 76] Tribunal de la protection des renseignements personnels et des données⁵ 	<ul style="list-style-type: none"> Commission d'accès à l'information du Québec (CAI) [41.1; 54] 	<ul style="list-style-type: none"> Commissariat à l'information et à la protection de la vie privée de l'Alberta (CIPVP de l'Alberta) [36] 	<ul style="list-style-type: none"> Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique (CIPVP de la C.-B.) [36] 	<ul style="list-style-type: none"> Autorité de contrôle de chaque État membre (CNIL en France, etc.) [51]
3. Champ d'application	<ul style="list-style-type: none"> Toute organisation qui recueille, utilise ou communique des renseignements personnels dans le cadre d'activités commerciales au Canada ou ayant un lien réel et substantiel avec le Canada⁶ [4] À l'exclusion des institutions fédérales auxquelles s'applique la <i>Loi sur la protection des renseignements personnels</i> [4(2)] Possibilité d'exclusion de l'application de la LPRPDE dans certaines provinces (Alberta, C.-B. et Québec) [26(2)] Ne concerne que les employés ou les candidats à un emploi dans une organisation qui recueille, utilise ou communique des renseignements personnels dans le cadre de l'exploitation d'une activité, d'une 	<ul style="list-style-type: none"> Toute organisation qui recueille, utilise ou communique des renseignements personnels dans le cadre d'activités commerciales au Canada, y compris : (1) à l'échelle interprovinciale ou internationale; ou (2) à l'échelle intraprovinciale, dans la mesure où l'organisation n'est pas assujettie à une ordonnance en vertu de la LPVPC déclarant qu'elle est assujettie à une loi provinciale qui est essentiellement similaire à la LPVPC [6(1)(2); 122(1)] À l'exclusion des institutions gouvernementales auxquelles s'applique la <i>Loi sur la protection des renseignements personnels</i> [6(4)a)] Possibilité d'exclusion de l'application de la LPVPC dans certaines provinces dotées d'une « loi sensiblement similaire » (lois applicables au secteur privé de l'Alberta, de la Colombie- 	<ul style="list-style-type: none"> Toute « entreprise » qui recueille, détient, utilise ou communique des renseignements personnels, que leur conservation soit assurée par l'entreprise ou par un tiers [1] À l'exclusion des organismes publics au sens de la <i>Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels</i> (c.-à-d. les organismes publics provinciaux du Québec) [3] 	<ul style="list-style-type: none"> Toute organisation qui recueille, utilise ou communique des renseignements personnels [3] À l'exclusion des « renseignements sur la santé » soumis à la <i>Health Information Act</i> de l'Alberta [4(3)] À l'exclusion des renseignements personnels soumis à la <i>Freedom of Information and Protection of Privacy Act</i> de l'Alberta (c.-à-d. les organismes publics provinciaux de l'Alberta) [4(3)] 	<ul style="list-style-type: none"> Toute organisation qui recueille, utilise ou communique des renseignements personnels [2] Exclut les renseignements personnels soumis à la LPRPDE Exclut les renseignements personnels soumis à la <i>Freedom of Information and Protection of Privacy Act</i> de la Colombie-Britannique (c.-à-d. les organismes publics provinciaux de la C.-B.) [3] 	<ul style="list-style-type: none"> Critère d'établissement : le responsable de traitement ou le sous-traitant doit être établi dans l'UE/EEE [3(1)] Critère de ciblage : le responsable de traitement est établi en dehors de l'UE/EEE, mais ses activités de traitement sont liées à l'offre de biens ou de services aux personnes concernées dans l'UE/EEE ou sont liées à la surveillance du comportement des personnes concernées dans l'UE/EEE [3(2)] Aucune distinction n'est faite entre le secteur privé et le secteur public [4(7)]

5. Le projet de loi C-27 édicterait aussi la *Loi sur le Tribunal de la protection des renseignements personnels et des données*, qui créerait le Tribunal de la protection des renseignements personnels et des données.

6. Les tribunaux canadiens appliquent le critère du « lien réel et substantiel » pour déterminer quand les tribunaux canadiens peuvent se déclarer compétents et, en pratique, les commissaires se sont déclarés compétents et ont appliqué les lois canadiennes sur la protection des renseignements personnels lorsqu'il y a relativement peu de facteurs de rattachement avec le Canada.

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)</i> ¹	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27</i> ²	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64</i> ³	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
	organisation ou d'une entreprise fédérale [4(1)b)]	Britannique et du Québec); lois applicables aux renseignements sur la santé de l'Ontario, du Nouveau-Brunswick, de Terre-Neuve-et-Labrador et de la Nouvelle-Écosse) [6(4)e)]				
4. Renseignements personnels (ou « données à caractère personnel »)	<ul style="list-style-type: none"> • Tout renseignement concernant un individu identifiable [2] • Quels que soient leur forme ou leur support • Régime particulier pour les « coordonnées d'affaires » (renseignements utilisés pour entrer en contact ou faciliter la prise de contact avec un individu dans le cadre de son emploi, c.-à-d. le nom, le poste, le titre, l'adresse du lieu de travail, le numéro de téléphone professionnel, etc.) [4.01] 	<ul style="list-style-type: none"> • Tout renseignement concernant un individu identifiable [2] • Quels que soient leur forme ou leur support • Les « renseignements personnels de tout individu que les organisations recueillent, utilisent ou communiquent <i>uniquement</i> pour entrer en contact — ou pour faciliter la prise de contact — avec lui dans le cadre de son emploi, de son entreprise ou de sa profession » n'entrent pas dans le champ d'application de la LPVPC [6(4)(d)] 	<ul style="list-style-type: none"> • Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier [2] • Quelle que soit la nature de son support et quelle que soit la forme sous laquelle ils sont accessibles (écrite, graphique, sonore, visuelle, informatisée ou autre) • Couvre également les employés et les candidats à un emploi • Régime particulier pour les « renseignements personnels qui concernent l'exercice par la personne concernée d'une fonction au sein d'une entreprise, tel que son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail » [1] 	<ul style="list-style-type: none"> • Tout renseignement qui concerne une personne physique identifiable [1(1)k)], y compris les « renseignements personnels de l'employé » • Exclut les « coordonnées d'affaires » recueillies, utilisées ou communiquées dans le but de permettre à une personne d'être jointe en rapport avec ses responsabilités professionnelles [4(3)] 	<ul style="list-style-type: none"> • Tout renseignement concernant une personne physique identifiable, y compris les « renseignements personnels de l'employé » [1] • Exclut les « coordonnées » et les « renseignements sur le produit du travail » [1] 	<ul style="list-style-type: none"> • Tout renseignement concernant une personne physique identifiée ou identifiable (y compris un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou un facteur propre à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale) [4(1)] • Quel que soit le support ou le format
5. Renseignements anonymisés	<ul style="list-style-type: none"> • Aucune définition pour les renseignements anonymisés 	<ul style="list-style-type: none"> • Les renseignements sont considérés comme anonymisés lorsqu'ils ne permettent plus 	<ul style="list-style-type: none"> • Les renseignements sont considérés comme anonymisés lorsqu'ils ne permettent plus, de 	<ul style="list-style-type: none"> • Pas de disposition précise 	<ul style="list-style-type: none"> • Pas de disposition précise 	<ul style="list-style-type: none"> • Les données à caractère personnel rendues anonymes de manière à ce

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques</i> (LPRPDE) ¹	<i>Loi sur la protection de la vie privée des consommateurs</i> (LPVPC), telle que proposée dans le projet de loi C-27 ²	<i>Loi sur la protection des renseignements personnels dans le secteur privé</i> , telle qu'amendée par le projet de loi 64 ³	<i>Personal Information Protection Act</i> de l'Alberta (PIPA de l'Alberta)	<i>Personal Information Protection Act</i> de la Colombie-Britannique (PIPA de la C.-B.)	<i>Règlement général sur la protection des données</i> (RGPD)
	<ul style="list-style-type: none"> • Toutefois, l'anonymisation peut être utilisée comme solution de rechange à la destruction ou à la suppression de renseignements personnels lorsqu'ils n'ont plus d'utilité [Ann. 1 – 4.5.3] 	<p>d'identifier directement ou indirectement un individu, et ce, de façon irréversible [2]</p> <ul style="list-style-type: none"> • Les renseignements doivent être anonymisés selon les meilleures pratiques généralement reconnues [2] • Le « retrait » renvoie à la suppression définitive et irréversible des renseignements personnels ou au fait de les <u>anonymiser</u> [2] • La LPVPC ne s'applique pas aux renseignements personnels qui ont été anonymisés [6(5)] 	<p>façon irréversible, d'identifier directement ou indirectement cette personne [23]</p> <ul style="list-style-type: none"> • Les renseignements doivent être anonymisés selon les meilleures pratiques généralement reconnues [23] • L'anonymisation est une solution de rechange à la destruction des renseignements personnels lorsque les fins auxquelles ils ont été recueillis ou utilisés sont accomplies, à condition que ces renseignements anonymisés soient utilisés à des fins sérieuses et légitimes [23] 			<p>que la personne concernée ne soit pas ou ne soit plus identifiable; qui ne sont pas soumis au RGPD [considérant 26]</p>
6. Renseignements dépersonnalisés	<ul style="list-style-type: none"> • Pas de définition de « renseignements dépersonnalisés » 	<ul style="list-style-type: none"> • Généralement, les renseignements dépersonnalisés sont des renseignements personnels qui ont été modifiés de manière à ce qu'un individu ne puisse pas être identifié directement, bien qu'un risque qu'il soit identifié demeure [2] • Les renseignements dépersonnalisés sont toujours considérés comme des renseignements personnels (avec exceptions) [2(3), voir 22(1); 39(1), 55; 56; 63(1); 71-75; 116] 	<ul style="list-style-type: none"> • Les renseignements dépersonnalisés sont des renseignements personnels qui ne permettent plus d'identifier directement la personne concernée [12] • Lors de l'utilisation de renseignements dépersonnalisés, des mesures raisonnables doivent être prises pour limiter les risques que quiconque procède à l'identification d'une personne physique à partir de renseignements dépersonnalisés [12] 	<ul style="list-style-type: none"> • Pas de disposition précise 	<ul style="list-style-type: none"> • Pas de disposition précise 	<ul style="list-style-type: none"> • Renseignements pseudonymisés - Données à caractère personnel traitées de telle manière qu'elles ne puissent plus être attribuées à une personne en particulier sans l'utilisation de renseignements supplémentaires conservés séparément, sous réserve de mesures techniques et organisationnelles [4(5)]; consiste en une mesure de sécurité et de protection des

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
						renseignements personnels dès la conception [25; 32]
7. Renseignements de nature sensible	<ul style="list-style-type: none"> • Pas de définition de « renseignements de nature sensible » • Recommandation visant à assurer un niveau de sécurité adapté au degré de sensibilité des renseignements [Ann. 1 – 4.7] 	<ul style="list-style-type: none"> • Les renseignements personnels d'un mineur sont considérés comme des renseignements de nature sensible [2(2)] • Le programme de gestion de la vie privée doit tenir compte de la sensibilité des renseignements [9(2)]; 62(1)] • Les périodes de conservation doivent être établies en fonction de la sensibilité des renseignements personnels [9(1)]; 53(2)] et, le cas échéant, les renseignements personnels doivent être rendus accessibles en prenant en compte leur nature sensible [62(2)e)] • La sensibilité des renseignements doit être prise en compte dans plusieurs autres situations [voir 12(2); 15(5); 22(b)(ii); 22(3)(a)(ii); 57(1); 58(8)(a); 74; 109(c)] 	<ul style="list-style-type: none"> • Les renseignements personnels sont considérés comme « sensibles » lorsqu'ils suscitent un haut degré d'attente raisonnable en matière de vie privée (cela inclut les renseignements médicaux, biométriques ou autrement intimes) [12] • Les mesures de sécurité doivent être raisonnables compte tenu de la sensibilité des renseignements [10] • Le consentement à l'utilisation ou à la communication de renseignements personnels de nature sensible doit être manifesté de façon expresse [12; 13] • La sensibilité des renseignements doit être prise en compte dans plusieurs autres situations [voir 3.3; 3.7; 17; 28.1; 90.2; 92.3] 	<ul style="list-style-type: none"> • Pas de définition de « renseignements de nature sensible » • En cas de consentement tacite, la collecte, l'utilisation ou la communication de renseignements personnels doit être raisonnable compte tenu de leur sensibilité [8(3)] 	<ul style="list-style-type: none"> • Pas de définition de « renseignements de nature sensible » • En cas de consentement tacite, la collecte, l'utilisation ou la communication de renseignements personnels doit être raisonnable compte tenu de leur sensibilité [8(3)] 	<ul style="list-style-type: none"> • Régime particulier pour les « catégories spéciales de données à caractère personnel » (y compris l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques, les données relatives à la santé, à la vie sexuelle ou à l'orientation sexuelle) [9] • Pas de régime distinct pour les données financières
8. Consentement	<ul style="list-style-type: none"> • Il peut être exprès ou tacite, selon les circonstances et le type de renseignements, considérant les attentes raisonnables de la personne concernée [Ann. 1 – 4.3.5] 	<ul style="list-style-type: none"> • Doit être obtenu préalablement ou au moment de la collecte des renseignements [15(1)(2)] • La personne concernée doit être informée, dans un langage clair, du type de renseignements personnels recueillis, utilisés et 	<ul style="list-style-type: none"> • Doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il doit être demandé à chacune de ces fins, en termes simples et clairs [14] 	<ul style="list-style-type: none"> • Peut être exprès ou tacite, chacun étant soumis à des exigences et à des limites précises [8] • Peut être retiré à tout moment moyennant un 	<ul style="list-style-type: none"> • Peut être exprès ou tacite, chacun étant soumis à des exigences et à des limites précises [7; 8] • Peut être retiré à tout moment moyennant un 	<ul style="list-style-type: none"> • Doit être librement donné, précis, éclairé et sans ambiguïté, sous une forme intelligible et accessible, et n'est valable qu'à des fins précises [4(11)]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
<ul style="list-style-type: none"> • Doit généralement être exprimé lors du traitement de renseignements sensibles [Ann. 1 – 4.3.6] • Peut être retiré à tout moment, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable [Ann. 1 – 4.3.8] • Une organisation peut recueillir, utiliser ou communiquer des renseignements personnels uniquement à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances [5(3)] 	<p>communiqués, ainsi que de la manière dont ils sont recueillis, des fins auxquelles ils sont recueillis, utilisés et communiqués, de même que des tiers auxquels les renseignements personnels pourraient être communiqués [15(3)(4)]</p> <ul style="list-style-type: none"> • Le consentement doit être donné expressément, sauf lorsqu'il est « approprié » de s'appuyer sur le consentement tacite, en tenant compte des attentes raisonnables de la personne et du degré de sensibilité des renseignements personnels [15(5)-15(6); 18] • Il peut être retiré à tout moment, en tout ou en partie, conformément à la LPVPC, à une loi fédérale ou provinciale applicable, ou aux conditions raisonnables d'un contrat [17] • Une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels que de la manière et à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances, que le consentement soit requis ou non aux termes de la LPVPC [12(1)] 	<ul style="list-style-type: none"> • Lorsque la demande de consentement est faite par écrit, elle doit être présentée distinctement de toute autre information communiquée à la personne concernée [14] • Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé [14] • Un consentement qui n'est pas donné conformément à la Loi est sans effet [14] • Le consentement à l'utilisation ou à la communication de renseignements personnels de nature sensible doit être manifesté de façon expresse [12; 13] • Le consentement à la communication ou à l'utilisation de renseignements personnels peut être retiré [8(4)] • Lorsqu'une personne est contactée à des fins de prospection commerciale ou philanthropique, cette personne doit être informée de son droit de retirer son consentement à ce que les renseignements personnels la concernant soient utilisés à ces fins [22] 	<p>préavis raisonnable, à moins que le retrait du consentement n'empêche l'exécution d'une obligation légale [9]</p>	<p>préavis raisonnable, à moins que le retrait du consentement n'empêche l'exécution d'une obligation légale [9]</p>	<ul style="list-style-type: none"> • Doit être « exprès » pour le traitement de catégories particulières de renseignements personnels [9(2)a)] • Peut être retiré à tout moment [7(3)]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
9. Exceptions applicables au consentement	<p><u>Collecte, utilisation et communication</u></p> <ul style="list-style-type: none"> • Non requis lorsque des exceptions s'appliquent (p. ex., dans le cas d'une « transaction commerciale éventuelle ») [7.2] 	<p><u>Collecte, utilisation et communication</u></p> <ul style="list-style-type: none"> - Non requis lorsque des exceptions s'appliquent, par exemple : <ul style="list-style-type: none"> - pour la collecte et l'utilisation de renseignements personnels pour certaines activités commerciales [15(6); 18] - pour la collecte et l'utilisation de renseignements personnels pour un intérêt légitime, sous réserve de multiples exigences, y compris la conduite d'une évaluation et la tenue de registres [18(3)(4)(5)] - pour l'intérêt public [29-39] - pour le transfert de renseignements personnels aux fournisseurs de services [2; 19] - pour les renseignements personnels dépersonnalisés, notamment dans le contexte d'une transaction commerciale potentielle [2; 20-22] - pour l'utilisation et la communication de renseignements personnels, dans le contexte d'une transaction commerciale, si la désidentification nuit aux objectifs de la transaction et si l'organisation a tenu compte du risque de préjudice pour l'individu que pourrait entraîner l'utilisation ou la communication 	<p><u>Utilisation</u></p> <ul style="list-style-type: none"> • Non requis lorsque des exceptions s'appliquent, par exemple lorsque les renseignements sont utilisés à des fins compatibles avec celles pour lesquelles ils ont été recueillis [12] <p><u>Communication</u></p> <ul style="list-style-type: none"> • Non requis lorsque des exceptions s'appliquent, par exemple lorsque les renseignements sont nécessaires aux fins de la conclusion d'une transaction commerciale [18.4] 	<p><u>Collecte, utilisation et communication</u></p> <ul style="list-style-type: none"> • Non requis lorsque des exceptions s'appliquent (p. ex., dans le cas d'une « transaction commerciale ») [22] 	<p><u>Collecte, utilisation et communication</u></p> <ul style="list-style-type: none"> • Non requis lorsque des exceptions s'appliquent (p. ex., dans le cas d'une « transaction commerciale ») [20] 	<p><u>Traitement</u></p> <ul style="list-style-type: none"> • Un autre motif juridique peut s'appliquer, comme la nécessité liée à l'exécution d'un contrat ou les fins légitimes du responsable de traitement [6(1)]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
		des renseignements personnels [22(2)]				
10. Enfants	<ul style="list-style-type: none"> Pas d'âge minimum pour le consentement des mineurs dans la LPRPDE, mais les Lignes directrices pour l'obtention d'un consentement valable du CPVPC mentionnent que le consentement doit généralement être obtenu auprès d'un parent ou d'un tuteur pour les enfants de moins de 13 ans 	<ul style="list-style-type: none"> Pas d'âge minimum pour le consentement des mineurs dans la LPVPC Les renseignements personnels d'un mineur sont considérés comme des renseignements de nature sensible [2(2)] Autres limites à la possibilité qu'ont les organisations à refuser de procéder au retrait des renseignements des mineurs [55(2)] Les parents peuvent agir au nom de leurs enfants pour protéger leurs droits [4] Le terme « mineur » n'est pas défini dans la LPVPC 	<ul style="list-style-type: none"> Le consentement pour la collecte de renseignements personnels <u>concernant un mineur de moins de 14 ans</u> doit être donné par le titulaire de l'autorité parentale, sauf lorsque cette collecte est manifestement au bénéfice de ce mineur [4.1; 14] Pour les mineurs âgés de <u>14 ans et plus</u>, le consentement peut également être donné directement par le mineur [14] 	<ul style="list-style-type: none"> Pas d'âge minimum pour le consentement des mineurs, mais ces derniers doivent être suffisamment âgés pour donner un consentement valable 	<ul style="list-style-type: none"> Pas d'âge minimum pour le consentement des mineurs, mais ces derniers doivent être suffisamment âgés pour donner un consentement valable 	<ul style="list-style-type: none"> L'âge minimum pour le consentement des mineurs est de 16 ans [8(1)] Les États membres peuvent prévoir un âge inférieur à 16 ans, à condition que cet âge ne soit pas inférieur à 13 ans [8(2)]
11. Programme de gouvernance	<ul style="list-style-type: none"> Les organisations doivent avoir des politiques et des pratiques concernant la gestion des renseignements personnels [Ann. 1 – 4.8.1] Les organisations doivent rendre accessibles au public les informations concernant leurs politiques et leurs pratiques concernant la gestion des renseignements personnels [Ann. 1 – 4.8; voir la section « Transparence »] 	<ul style="list-style-type: none"> Toute organisation doit mettre en œuvre et maintenir un programme de gestion de la protection des renseignements personnels qui comprend les politiques, les pratiques et les procédures qu'elle a mises en place pour se conformer aux obligations qui lui incombent en vertu de la LPVPC, notamment des politiques, des pratiques et des procédures concernant : <ul style="list-style-type: none"> la protection des renseignements personnels 	<ul style="list-style-type: none"> Chaque entreprise doit établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance visant à assurer la protection des renseignements personnels [3.2] Ces politiques et pratiques doivent notamment fournir un cadre concernant : <ul style="list-style-type: none"> la conservation et la destruction des renseignements 	<ul style="list-style-type: none"> Chaque organisation doit élaborer et suivre des politiques et des pratiques qui sont raisonnables, afin que l'organisation puisse s'acquitter des obligations qui lui incombent en vertu de la PIPA de l'Alberta [6(1)] 	<ul style="list-style-type: none"> Chaque organisation doit : <ul style="list-style-type: none"> élaborer et suivre des politiques et pratiques nécessaires pour lui permettre de s'acquitter des obligations qui lui incombent en vertu de la PIPA de la C.-B. [5] élaborer un processus pour lui permettre de répondre aux plaintes qui pourraient survenir 	<ul style="list-style-type: none"> Le responsable de traitement met en œuvre les politiques appropriées pour la protection des données [24(2)] Le délégué à la protection des données (voir la section « responsable de la protection des renseignements personnels ») doit examiner les politiques du responsable de traitement en matière de protection

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques</i> (LPRPDE) ¹	<i>Loi sur la protection de la vie privée des consommateurs</i> (LPVPC), telle que proposée dans le projet de loi C-27 ²	<i>Loi sur la protection des renseignements personnels dans le secteur privé</i> , telle qu'amendée par le projet de loi 64 ³	<i>Personal Information Protection Act de l'Alberta</i> (PIPA de l'Alberta)	<i>Personal Information Protection Act de la Colombie-Britannique</i> (PIPA de la C.-B.)	<i>Règlement général sur la protection des données</i> (RGPD)
		<ul style="list-style-type: none"> - la réception et le traitement des demandes de renseignements et des plaintes - la formation et les informations fournies au personnel de l'organisation relativement à ses politiques, pratiques et procédures - l'élaboration de documents pour expliquer les politiques et les procédures de l'organisation [9; 62] • Les organisations doivent rendre facilement accessibles, dans un langage clair, les informations concernant leurs politiques et pratiques [62(1); voir la section « Transparence »] 	<ul style="list-style-type: none"> - les rôles et les responsabilités des membres du personnel tout au long du cycle de vie de ces renseignements - le processus de traitement des plaintes relatives à la protection des renseignements [3.2] • Chaque entreprise doit publier des informations détaillées au sujet de ces politiques, en termes clairs et simples, sur son site Internet [3.2] 		relativement à l'application de la PIPA de la C.-B. [5]	des données à caractère personnel, notamment : <ul style="list-style-type: none"> - l'attribution des responsabilités - le travail de sensibilisation - la formation du personnel affecté aux activités de traitement - les audits connexes [39(1)]
12. Droit d'accès	<ul style="list-style-type: none"> • Oui, sous réserve de certaines exceptions et interdictions concernant la communication Les exceptions comprennent les situations lors desquelles les renseignements sont protégés par le secret professionnel liant l'avocat à son client et lors desquelles les renseignements contiennent des références à des tiers ou ne peuvent être divulgués pour des raisons d'ordre juridique, des raisons de sécurité ou des raisons d'ordre commercial [9; Ann. 1-4.9] • Demande d'accès par écrit [8(1)] 	<ul style="list-style-type: none"> • Oui, sous réserve de certaines exceptions et d'interdiction de la communication Les exceptions comprennent le cas où le fait de donner accès révélerait des renseignements commerciaux confidentiels ou pourrait menacer la vie ou la sécurité d'un autre individu [70(7)] • Demande d'accès écrite [64(1)] • Réponse dans les 30 jours (ce délai peut être prolongé de 30 jours dans certains cas) [67] • Des droits peuvent être exigés dans certaines conditions [68] 	<ul style="list-style-type: none"> • Oui, sous réserve de certaines exceptions, notamment en cas de litige ou s'il y a un risque de porter gravement préjudice à un tiers [27; 37 et paragraphes afférents] • Demandes d'accès par écrit, appuyées par une preuve d'identité et adressées au responsable de la protection des renseignements personnels [30] • Réponse écrite dans les 30 jours; aucune possibilité de prolonger le délai de 30 jours [32] 	<ul style="list-style-type: none"> • Oui, sous réserve de certaines exceptions, notamment lorsque les renseignements sont protégés par un privilège juridique ou que leur divulgation pourrait révéler des renseignements personnels sur une autre personne ou menacer sa vie ou sa sécurité [24] • Demande d'accès par écrit • Réponse dans un délai de 45 jours civils (ce 	<ul style="list-style-type: none"> • Oui, sous réserve de certaines exceptions, notamment lorsque les renseignements sont protégés par le secret professionnel ou que leur divulgation pourrait révéler des renseignements personnels sur une autre personne ou menacer sa santé ou sa sécurité [23] • Demande d'accès par écrit • Réponse dans les 30 jours ouvrables (ce délai peut être prolongé) 	<ul style="list-style-type: none"> • Oui, sous réserve de certaines exceptions, y compris pour des raisons juridiques ou de sécurité [15; 23] • En cas de doute raisonnable sur l'identité de la personne concernée, il est possible de demander une confirmation de son identité [12(6)] • Réponse donnée par écrit ou verbalement (à la demande de la personne concernée) [12(1)] • La réponse doit être donnée sans retard

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
	<ul style="list-style-type: none"> • Réponse dans les 30 jours (ce délai peut être prolongé de 30 jours dans certains cas) [8(3)] • Des droits peuvent être exigés sous certaines conditions [8(6)] • Sur requête de l'individu, l'organisation fournit à celui-ci l'aide dont il a besoin pour préparer sa demande [8(2)] 	<ul style="list-style-type: none"> • Sur requête de l'individu, l'organisation lui fournit l'aide dont il a besoin pour préparer sa demande [64(2)] 	<ul style="list-style-type: none"> • L'entreprise a l'obligation de fournir une assistance [27; 29; 30] • Gratuit (des frais raisonnables peuvent être exigés dans certaines conditions) [33] • En cas de refus, la personne responsable de la protection des renseignements personnels doit indiquer les raisons du refus et les dispositions de la loi sur lesquelles le refus s'appuie, ainsi que les recours qui s'offrent au requérant et le délai dans lequel ils peuvent être exercés. Doit également aider le requérant à comprendre le refus [34] • Obligations particulières pour les renseignements personnels informatisés [27]⁷ • L'entreprise doit informer la personne de son droit d'accès lorsque ses renseignements personnels sont recueillis [8] 	<p>délai peut être prolongé)</p> <ul style="list-style-type: none"> • Des frais peuvent être exigés dans certaines conditions • Une organisation doit faire tous les efforts raisonnables pour aider le demandeur 	<ul style="list-style-type: none"> • Des frais peuvent être exigés dans certaines conditions • Une organisation doit faire un effort raisonnable pour aider le demandeur 	<p>excessif et dans tous les cas dans un délai d'un (1) mois (ce délai peut être prolongé) [12(3)]</p> <ul style="list-style-type: none"> • Gratuit (des frais raisonnables peuvent être exigés, sous certaines conditions) [12(5)] : <ul style="list-style-type: none"> - Obligation de faciliter l'exercice des droits d'accès [12(2)]
13. Droit de corriger (ou de rectifier)	<ul style="list-style-type: none"> • Oui, si les renseignements sont inexacts ou incomplets [Ann. 1 – 4.9.5] 	<ul style="list-style-type: none"> • Oui, si la personne démontre que les renseignements sont désuets, inexacts ou incomplets, l'organisation doit les modifier [71(1)] 	<ul style="list-style-type: none"> • Oui, si les renseignements sont inexacts, incomplets ou équivoques, ou si la collecte, la communication ou la conservation des 	<ul style="list-style-type: none"> • Oui, s'il y a une erreur ou une omission dans les renseignements personnels [25] 	<ul style="list-style-type: none"> • Oui, s'il y a une erreur ou une omission dans les renseignements personnels [24] 	<ul style="list-style-type: none"> • Oui, si les données sont inexacts ou incomplètes [16] • Les exigences en matière de droit d'accès

7. Le droit relatif à la « transférabilité » des données entrera en vigueur le 22 septembre 2024.

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
		<ul style="list-style-type: none"> L'organisme doit, s'il y a lieu, transmettre les renseignements modifiés à toute partie y ayant accès [71(2)] 	<p>renseignements n'est pas autorisée par la loi [28]</p> <ul style="list-style-type: none"> Les exigences en matière de droit d'accès s'appliquent avec les modifications nécessaires 	<ul style="list-style-type: none"> Demande de rectification par écrit Les renseignements doivent être rectifiés dès que cela est raisonnablement possible Aucuns frais ne peuvent être perçus 	<ul style="list-style-type: none"> Demande de rectification par écrit Les renseignements doivent être rectifiés dès que cela est raisonnablement possible Aucuns frais ne peuvent être perçus Si la rectification est refusée, le dossier doit être annoté 	s'appliquent avec les modifications nécessaires
14. Droit à l'effacement (ou « droit à l'oubli »)	<ul style="list-style-type: none"> Non 	<ul style="list-style-type: none"> Ce droit est dans une certaine mesure prévu dans la LPVPC, particulièrement pour retirer des renseignements personnels qui concernent une personne (sous réserve de certaines conditions et exceptions) et pour exiger que l'organisation informe tout fournisseur de services à qui elle a pu transférer ces renseignements, et pour confirmer que celui-ci a procédé à leur retrait [55] Aucun droit formel de désindexer ou de réindexer un lien hypertexte à la demande d'une personne 	<ul style="list-style-type: none"> Oui, pour faire cesser la diffusion des renseignements, désindexer ou réindexer tout hyperlien rattaché au nom de la personne concernée et donnant accès aux renseignements par un moyen technologique [28.1] Seulement lorsque la diffusion contrevient à la loi ou lorsque certaines conditions sont réunies [28.1] Demandes d'accès par écrit, appuyées par une preuve d'identité et adressées au responsable de la protection des renseignements personnels [30] Réponse écrite dans les 30 jours [32] 	<ul style="list-style-type: none"> Non 	<ul style="list-style-type: none"> Non 	<ul style="list-style-type: none"> Oui (sous certaines conditions) [17]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
			<ul style="list-style-type: none"> • L'entreprise a l'obligation de fournir une assistance [30] • En cas de refus, la personne responsable de la protection des renseignements personnels doit indiquer les raisons du refus et les dispositions de la loi sur lesquelles le refus s'appuie, ainsi que les recours qui s'offrent au requérant et le délai dans lequel ils peuvent être exercés. Doit également aider le requérant à comprendre le refus [34] 			
15. Autres droits des particuliers	<ul style="list-style-type: none"> • Droit d'adresser à l'organisation une contestation concernant la non-conformité à la LPRPDE [Ann. 1 – 4.10] • Droit de déposer une plainte auprès du CPVP [11(1)] 	<ul style="list-style-type: none"> • Droit de déposer une plainte auprès de l'organisation [73] • Droit de déposer une plainte auprès du CPVP [82] • Droit d'être informé si un système décisionnel automatisé a été utilisé pour faire la prédiction, prendre la décision ou faire la recommandation qui a une incidence importante sur l'individu [63(3)] • Droit à la transférabilité des données personnelles lorsque les deux organisations sont soumises à un « cadre de mobilité des données » [72; 123] 	<ul style="list-style-type: none"> • Droit de déposer une plainte auprès de l'entreprise [3.2] • Droit de déposer une plainte auprès de la CAI [81] • Droit de soumettre une demande à la CAI pour l'examen d'une mésentente [42] • Droit d'être informé si une décision rendue est fondée exclusivement sur un traitement automatisé des renseignements personnels, de présenter des observations et de demander une révision de cette décision [12.1] • Droit d'obtenir les renseignements personnels dans un format technologique structuré et couramment utilisé, 	<ul style="list-style-type: none"> • Droit de déposer une plainte auprès du CIPVP de l'Alberta ou de demander la révision de la décision d'une organisation relativement à la demande d'une personne au sujet des renseignements personnels [36] 	<ul style="list-style-type: none"> • Droit de déposer une plainte auprès de l'organisation [46] • Droit de déposer une plainte auprès du CIPVP de la C.-B. ou de demander la révision d'une décision prise par une organisation concernant la demande d'accès ou de rectification des renseignements personnels d'une personne [47] 	<ul style="list-style-type: none"> • Droit de déposer une plainte auprès de l'autorité de contrôle compétente [77] • Droit à la limitation du traitement des renseignements personnels [18] • Droit à la transférabilité des renseignements personnels [20] • Droit de s'opposer au traitement des renseignements personnels [21] • Droit de ne pas faire l'objet d'une décision fondée uniquement sur un traitement automatisé [22]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
			et de les faire communiquer, sur requête du demandeur, à toute personne ou à tout organisme autorisé par la loi à recueillir de tels renseignements [27]			
16. Responsable de la protection de la vie privée	<ul style="list-style-type: none"> Obligation de désigner une personne responsable du respect de la LPRPDE et de communiquer l'identité de cette personne [Ann. 1 – 4.1] 	<ul style="list-style-type: none"> Obligation de désigner un ou plusieurs individus chargés de la conformité de l'organisation à la LPVPC [8(1)] Les coordonnées d'affaires des individus désignés doivent être fournies à quiconque en fait la demande [8(1)] Les individus désignés ne sont pas nécessairement les individus à qui les plaintes et les demandes en vertu de la LPVPC sont acheminées [62(2)(g) lu avec 8(1)] 	<ul style="list-style-type: none"> Il incombe à la personne ayant la plus haute autorité de veiller à ce que la Loi soit appliquée et respectée [3.1] Cette fonction pourra être déléguée, par écrit, à toute autre personne [3.1] Cette personne doit approuver les politiques et pratiques de l'entreprise [3.2] Cette personne doit être consultée pour toute évaluation des facteurs relatifs à la vie privée (EFVP) [3.3] Cette personne peut proposer toute mesure de protection des renseignements personnels applicable à un projet d'acquisition, de développement ou de restructuration d'un système d'information [3.4] Cette personne doit être consultée lors de l'évaluation du risque de préjudice pour une personne dont les renseignements personnels sont liés à un incident de confidentialité [3.7] 	<ul style="list-style-type: none"> L'organisation doit désigner une ou plusieurs personnes responsables du respect de la PIPA de l'Alberta [5(3)] 	<ul style="list-style-type: none"> L'organisation doit désigner une ou plusieurs personnes responsables du respect de la PIPA de la C.-B., et mettre à disposition le nom ou le titre du poste et les coordonnées de chacune de ces personnes [4(3)] 	<ul style="list-style-type: none"> Obligation de désigner un « délégué à la protection des données » dans certaines circonstances, dont le traitement à grande échelle de catégories particulières de données ou les activités de traitement qui nécessitent un suivi régulier et systématique des personnes concernées à grande échelle [37]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques</i> (LPRPDE) ¹	<i>Loi sur la protection de la vie privée des consommateurs</i> (LPVPC), telle que proposée dans le projet de loi C-27 ²	<i>Loi sur la protection des renseignements personnels dans le secteur privé</i> , telle qu'amendée par le projet de loi 64 ³	<i>Personal Information Protection Act de l'Alberta</i> (PIPA de l'Alberta)	<i>Personal Information Protection Act de la Colombie-Britannique</i> (PIPA de la C.-B.)	<i>Règlement général sur la protection des données</i> (RGPD)
			<ul style="list-style-type: none"> Cette personne est responsable des demandes d'accès, de rectification ou de suppression [28.1; 30; 32; 34; 35] 			
17. Transparence	<ul style="list-style-type: none"> Les organisations doivent rendre facilement accessibles à toute personne, sous une forme généralement compréhensible, les politiques et pratiques relatives à la gestion des renseignements personnels [Ann. 1 – 4.8] Les organisations doivent informer les personnes concernées du genre de renseignements personnels qu'elles possèdent et fournir une explication générale de l'usage auquel ils sont destinés [Ann. 1 – 4.8] Les organisations doivent être en mesure d'expliquer aux personnes concernées les raisons pour lesquelles les renseignements sont recueillis [Ann. 1 – 4.8] 	<ul style="list-style-type: none"> Les organisations doivent rendre facilement accessibles, dans un langage clair, des renseignements expliquant leurs politiques et leurs pratiques [9; 62(1)], dont : <ul style="list-style-type: none"> la description du type de renseignements personnels qui relèvent de l'organisation une explication générale de l'usage qui est fait des renseignements personnels et de la façon dont l'organisation applique les exceptions de consentement une explication générale de l'usage que l'organisation fait des systèmes décisionnels automatisés qui pourraient avoir une incidence importante sur les individus concernés le fait que l'organisation effectue ou non des communications ou des transferts interprovinciaux ou internationaux qui pourraient avoir des répercussions raisonnablement prévisibles sur la vie privée des individus concernés 	<ul style="list-style-type: none"> Les entreprises doivent publier des informations détaillées sur leurs politiques et leurs pratiques en termes simples et clairs [3.2] Si des renseignements personnels sont recueillis par un moyen technologique, l'entreprise doit publier sur son site Internet une politique de confidentialité rédigée en termes clairs et simples [8.2] Pour obtenir un consentement valide [8.3], les entreprises doivent informer les personnes, préalablement ou lors de la collecte de renseignements personnels, à propos : <ul style="list-style-type: none"> des fins auxquelles ces renseignements sont recueillis des moyens par lesquels les renseignements sont recueillis du droit d'accès et du droit de rectification 	<ul style="list-style-type: none"> Les organisations doivent fournir sur demande des informations sur leurs politiques et pratiques en matière de conformité à la PIPA de l'Alberta, y compris sur leur recours à des fournisseurs de services à l'étranger pour la collecte, l'utilisation, la communication ou la conservation de renseignements personnels [6] 	<ul style="list-style-type: none"> Les organisations doivent fournir sur demande des informations sur leurs politiques et pratiques en matière de conformité à la PIPA de la C.-B., et sur leurs procédures de traitement des plaintes [5] 	<ul style="list-style-type: none"> Les organisations doivent fournir à la personne concernée une grande variété d'informations au moment où les données sont obtenues (fins pour lesquelles elles sont traitées, fondements juridiques, destinataires, transfert des données, durée du stockage, droits applicables, coordonnées du responsable de traitement ou du délégué à la protection des données, etc.) [13] Lorsque des données à caractère personnel n'ont pas été obtenues auprès de la personne concernée, des informations (dont l'identité du responsable de traitement, les destinataires des données à caractère personnel, etc.) doivent être fournies [14] Tout renseignement doit être fourni sous une forme concise, transparente,

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
	<ul style="list-style-type: none"> - les périodes de conservation établies pour les renseignements personnels de nature sensible - les droits de retrait et d'accès - les coordonnées d'affaires de l'individu à qui les plaintes ou les demandes de renseignements peuvent être acheminées [62(2)] • Pour obtenir un consentement valide, les organisations doivent informer les individus concernés en langage clair, préalablement ou au moment de la collecte, de ce qui suit : <ul style="list-style-type: none"> - les fins de la collecte, de l'utilisation ou de la communication des renseignements personnels - la manière dont les renseignements personnels seront recueillis, utilisés ou communiqués - les conséquences raisonnablement prévisibles de la collecte, de l'utilisation et de la communication des renseignements personnels - le type précis de renseignements personnels que l'organisation recueillera, utilisera ou communiquera - le nom des tiers ou les catégories de tiers auxquels les renseignements personnels pourraient être communiqués [15(3)] 	<ul style="list-style-type: none"> - du droit de retirer leur consentement - du nom du tiers pour qui les renseignements sont recueillis (le cas échéant) - du nom des tiers ou des catégories de tiers à qui ces renseignements seront communiqués par nécessité - de la possibilité que les renseignements soient communiqués à l'extérieur du Québec [8] - de l'utilisation d'une technologie qui comprend des fonctions permettant d'identifier, de localiser ou d'effectuer un profilage, en plus de l'informer des moyens offerts pour activer ces fonctions [8.1] • Au plus tard au moment où une personne est informée d'une décision fondée exclusivement sur un traitement automatisé, les entreprises doivent l'informer de l'utilisation de cette technologie de manière appropriée [12.1] • Les entreprises doivent publier sur leur site Internet le titre et les coordonnées de la personne responsable de la protection des renseignements personnels ou, si l'entreprise n'a pas de site Internet, rendre 			<p>intelligible et facilement accessible, en utilisant un langage clair et simple [12(1)]</p>

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
			<p>ces informations accessibles par tout autre moyen approprié</p> <ul style="list-style-type: none"> • Les entreprises doivent porter à la connaissance du public l'endroit où les renseignements personnels sont accessibles et les moyens d'y accéder [29] • Lorsque des renseignements personnels sont utilisés à des fins de prospection commerciale ou philanthropique, la personne doit s'identifier et informer la personne concernée de son droit de retirer son consentement à ce que les renseignements personnels la concernant soient utilisés à ces fins [22] 			
18. Mesures de sécurité	<ul style="list-style-type: none"> • Les organisations doivent mettre en œuvre des mesures de sécurité, y compris des moyens matériels, des mesures administratives et des mesures technologiques, en fonction du degré de sensibilité des renseignements, de la quantité, de la répartition et du format des renseignements, ainsi que de la méthode de conservation [Ann. 1 – 4.7] • Obligation de sensibiliser les employés à l'importance de protéger le caractère confidentiel des renseignements personnels [Ann. 1 – 4.7.4] 	<ul style="list-style-type: none"> • Les organisations protègent les renseignements personnels au moyen de mesures de sécurité matérielles, organisationnelles et techniques. Le degré de protection des renseignements personnels est proportionnel à la mesure dans laquelle les renseignements sont de nature sensible [57] 	<ul style="list-style-type: none"> • Les entreprises doivent mettre en œuvre les mesures de sécurité propres à assurer une protection des renseignements personnels qui sont raisonnables compte tenu de la sensibilité des renseignements, de la finalité de leur utilisation, de leur quantité et de leur répartition et du support sur lequel ils sont conservés [10] 	<ul style="list-style-type: none"> • Les organisations doivent prendre des mesures de sécurité raisonnables contre des risques comme l'accès, la collecte, l'utilisation, la communication, la copie, la modification, la suppression ou la destruction non autorisés [34] 	<ul style="list-style-type: none"> • Les organisations doivent prendre des mesures de sécurité raisonnables pour empêcher l'accès, la collecte, l'utilisation, la communication, la copie, la modification, la suppression non autorisée ou tout autre risque similaire [34] 	<ul style="list-style-type: none"> • Les organisations doivent mettre en œuvre des mesures techniques et organisationnelles pour assurer un niveau de sécurité adapté au risque (y compris la pseudonymisation et le cryptage des données, le cas échéant) [32]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
19. Définition d'« atteinte aux mesures de sécurité »	<ul style="list-style-type: none"> • Une atteinte aux mesures de sécurité s'entend d'une communication non autorisée ou d'une perte de renseignements personnels, ou d'un accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation [2(1)] 	<ul style="list-style-type: none"> • Une atteinte aux mesures de sécurité s'entend d'une communication non autorisée ou d'une perte de renseignements personnels, ou d'un accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation [2(1)] 	<ul style="list-style-type: none"> • Un « incident de confidentialité » s'entend : <ul style="list-style-type: none"> - d'un accès non autorisé par la loi à des renseignements personnels - d'une utilisation non autorisée par la loi des renseignements personnels - d'une communication non autorisée par la loi des renseignements personnels - de la perte des renseignements personnels - de toute autre atteinte à la protection de tels renseignements [3.6] 	<ul style="list-style-type: none"> • Un incident de confidentialité s'entend d'une communication non autorisée ou d'une perte de renseignements personnels, ou d'un accès non autorisé à ceux-ci [34.1] 	<ul style="list-style-type: none"> • s. o. 	<ul style="list-style-type: none"> • Une atteinte aux données à caractère personnel est une atteinte à la sécurité qui entraîne la destruction accidentelle ou illégale, la perte, l'altération ou la communication non autorisée de données à caractère personnel, ou l'accès non autorisé à de telles données qui ont été transmises, stockées ou traitées autrement [4(12)]
20. Signalement d'une atteinte	<ul style="list-style-type: none"> • Signalement obligatoire au CPVP, dès que possible, de toute atteinte présentant un « risque réel de préjudice grave » [10.1] • Signalement obligatoire à l'intéressé, dès que possible, de toute atteinte présentant un « risque réel de préjudice grave » [10.1(3)] • Signalement obligatoire à toute autre organisation ou toute institution gouvernementale ou subdivision d'une telle institution qui pourrait réduire le risque [10.2] • Conserver un registre de toutes les atteintes à la protection des 	<ul style="list-style-type: none"> • Signalement obligatoire au CPVP, dès que possible, de toute atteinte présentant un « risque réel de préjudice grave » [58] • Signalement obligatoire à l'individu, dès que possible, de toute atteinte présentant un « risque réel de préjudice grave » [58] • Signalement obligatoire à toute autre organisation, institution gouvernementale ou subdivision d'une telle institution qui pourrait réduire le risque [59] • Obligation de tenir et de conserver un registre de toutes les atteintes à la protection de données et, sur 	<ul style="list-style-type: none"> • Signalement obligatoire à la CAI de tout incident qui présente un risque de préjudice sérieux [3.5] • Signalement obligatoire à toute personne dont les renseignements personnels sont concernés par l'incident de confidentialité créant un risque de préjudice sérieux, sauf si cela serait susceptible d'entraver une enquête [3.5] • Signalement discrétionnaire à toute personne ou à tout organisme susceptible de réduire le risque [3.5] • Obligation de conserver et de tenir à jour un registre de 	<ul style="list-style-type: none"> • Signalement obligatoire au CIPVP de l'Alberta, dès que possible, de tout accès non autorisé à des renseignements personnels ou de toute divulgation de ceux-ci créant un « risque réel de préjudice grave » [34.1] • Le CIPVP de l'Alberta peut exiger un signalement aux personnes qui courent un « risque réel de préjudice grave » [<i>Personal Information Protection Act Regulation</i>] 	<ul style="list-style-type: none"> • Aucune exigence • Signalement facultatif au CIPVP de la C.-B. 	<ul style="list-style-type: none"> • Signalement obligatoire à l'autorité de contrôle sans retard injustifié et, si possible, au plus tard 72 heures après avoir eu connaissance de l'incident dans certaines circonstances [33] • Obligation de communiquer avec la personne concernée sans retard injustifié lorsque la violation des données est susceptible d'entraîner un risque élevé pour les droits et libertés, sous certaines conditions [33]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques</i> (LPRPDE) ¹	<i>Loi sur la protection de la vie privée des consommateurs</i> (LPVPC), telle que proposée dans le projet de loi C-27 ²	<i>Loi sur la protection des renseignements personnels dans le secteur privé</i> , telle qu'amendée par le projet de loi 64 ³	<i>Personal Information Protection Act de l'Alberta</i> (PIPA de l'Alberta)	<i>Personal Information Protection Act de la Colombie-Britannique</i> (PIPA de la C.-B.)	<i>Règlement général sur la protection des données</i> (RGPD)
	données et, sur demande, donner au CPVP accès à ce registre [10.3]	demande, de donner au CPVP accès à ce registre [60] <ul style="list-style-type: none"> Les fournisseurs de services doivent signaler toute atteinte à la sécurité des renseignements personnels à l'organisation de laquelle ils relèvent [61] 	chaque incident de confidentialité pendant les cinq années suivant l'incident et, sur demande, donner à la CAI accès au registre [3.8] <ul style="list-style-type: none"> Un règlement détermine le contenu et les modalités des avis et du registre des incidents de confidentialité [3.5; 3.8] Si une entreprise a des motifs de croire qu'il s'est produit un incident de confidentialité, elle doit prendre les mesures raisonnables pour réduire les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent [3.5] 			
21. Transfert permis vers des territoires étrangers	<ul style="list-style-type: none"> À l'extérieur du Canada Oui, par voie contractuelle ou autre, à condition qu'un degré comparable de protection soit assuré pour les renseignements personnels [4.1.3] Les personnes doivent être informées que leurs renseignements peuvent être envoyés vers un pays étranger à des fins de traitement et qu'ils peuvent être accessibles aux tribunaux et aux autorités chargées de l'application de la loi et de la sécurité nationale de 	<ul style="list-style-type: none"> À l'extérieur du Canada Oui, tant que l'organisation informe l'individu qu'elle effectue un transfert international ou interprovincial de renseignements personnels pouvant avoir des répercussions raisonnablement prévisibles sur la vie privée [62(2)d)] À un « fournisseur de services » [2], à l'insu de l'individu concerné et sans son consentement, si l'organisation s'assure, par contrat ou autrement, que le fournisseur de services offre un degré de 	<ul style="list-style-type: none"> À l'extérieur du Québec Oui, après la conduite d'une EFVP, en tenant compte : <ul style="list-style-type: none"> de la sensibilité des renseignements des fins auxquelles ils seront utilisés; des mesures de protection applicables, y compris les mesures contractuelles du régime juridique applicable dans l'État où les renseignements seraient communiqués, notamment les 	<ul style="list-style-type: none"> À l'extérieur de l'Alberta Oui, mais si une organisation utilise un fournisseur de services à l'extérieur du Canada pour recueillir, utiliser, communiquer ou stocker des renseignements personnels, alors la politique de confidentialité doit inclure des renseignements concernant : 	<ul style="list-style-type: none"> À l'extérieur de la Colombie-Britannique Oui, mais la mention dans la politique de confidentialité est recommandée par le CIPVP de la C.-B. 	<ul style="list-style-type: none"> À l'extérieur de l'UE/EEE Oui, s'il existe une « décision d'adéquation » ou d'autres garanties appropriées dans le cadre du RGPD, comme des clauses contractuelles types approuvées par la Commission européenne, des règles d'entreprise contraignantes, l'adhésion à un code de conduite ou un mécanisme de certification [44 à 47]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
	<p>ce pays [conformément aux lignes directrices sur le transfert transfrontalier de renseignements personnels]</p> <ul style="list-style-type: none"> Le CPVP peut communiquer des renseignements à un État étranger dans des conditions précises [23.1] 	<p>protection des renseignements personnels équivalent à celui que l'organisation est tenue d'offrir en vertu de la LPVPC [7; 11]</p> <ul style="list-style-type: none"> Le CPVP peut communiquer des renseignements à un État étranger dans des conditions précises [120] 	<p>principes de protection des données qui y sont applicables [17]</p> <ul style="list-style-type: none"> Les renseignements personnels peuvent être communiqués si l'EFVP qu'ils bénéficieront d'une protection adéquate au regard des principes de protection des renseignements personnels généralement reconnus [17] La communication des renseignements doit faire l'objet d'une entente écrite [17] 	<ul style="list-style-type: none"> les États à l'extérieur du Canada où la collecte, l'utilisation, la communication ou le stockage peuvent avoir lieu les fins auxquelles le fournisseur de services à l'extérieur du Canada a été autorisé à recueillir, à utiliser ou à communiquer des renseignements personnels [6(2)] 	<ul style="list-style-type: none"> Avant les garanties appropriées, évaluation des risques liés aux transferts [Schrems II] Obligation de désigner un « représentant » dans un contexte extraterritorial, si aucun établissement n'est établi dans l'UE mais que le marché de l'UE est ciblé [27] Quelques exceptions aux exigences relatives à la décision d'adéquation et aux garanties appropriées, applicables à des situations précises [49] 	
22. Confidentialité dès la conception	<ul style="list-style-type: none"> Aucune exigence formelle. Cependant, une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances [5(3)] La collecte, l'utilisation et la communication des renseignements personnels doivent se limiter aux fins que l'organisation a déterminées [Ann. 1; 4.4; 4.5] 	<ul style="list-style-type: none"> Aucune exigence formelle. Cependant, une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels que de la manière et à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances, que le consentement soit requis ou non aux termes de la LPVPC [12(1)] Une organisation ne peut recueillir que les renseignements personnels nécessaires aux fins qu'elle a déterminées et enregistrées avant la collecte et ne peut utiliser ou communiquer des renseignements personnels qu'à ces fins, avec le consentement valide de la personne concernée 	<ul style="list-style-type: none"> Si l'entreprise offre au public des produits ou des services technologiques disposant de paramètres de confidentialité, ces paramètres doivent, par défaut, assurer le plus haut niveau de confidentialité (à l'exception des paramètres de confidentialité des témoins de connexion) [9.1] 	<ul style="list-style-type: none"> Aucune exigence formelle. La LPVPC prévoit qu'une organisation peut recueillir, utiliser ou communiquer des renseignements personnels uniquement à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances, après avoir tenu compte de certains éléments énumérés dans la LPVPC. 	<ul style="list-style-type: none"> Aucune exigence formelle. La LPVPC prévoit qu'une organisation peut recueillir, utiliser ou communiquer des renseignements personnels uniquement à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances, après avoir tenu compte de certains éléments énumérés dans la LPVPC. 	<ul style="list-style-type: none"> Le responsable de traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées (telles que la pseudonymisation) conçues pour mettre en œuvre de manière efficace les principes de protection des données comme la minimisation des données et pour intégrer les garanties nécessaires au traitement, de manière à satisfaire aux exigences du RGPD et de protéger les droits des personnes concernées [25(1)]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
		ou dans les circonstances prévues par la LPVPC [13; 14]				
23. Nouveaux projets liés aux renseignements personnels	<ul style="list-style-type: none"> Aucune exigence précise Recommandation du CPVP 	<ul style="list-style-type: none"> Aucune exigence précise Recommandation du CPVP 	<ul style="list-style-type: none"> Les entreprises doivent effectuer une EFVP pour tout projet d'acquisition, de développement et de refonte d'un système d'information [3.3] 	<ul style="list-style-type: none"> Aucune exigence précise concernant une EFVP Recommandation du CIPVP de l'Alberta 	<ul style="list-style-type: none"> Aucune exigence précise concernant une EFVP Recommandation du CIPVP de la C.-B. 	<ul style="list-style-type: none"> L'évaluation des facteurs relatifs à la protection des données est requise dans certaines circonstances [35]
24. Vérifications	<ul style="list-style-type: none"> Le CPVP peut, sur préavis suffisant et à toute heure convenable, procéder à la vérification des pratiques de l'organisation en matière de gestion des renseignements personnels s'il a des motifs raisonnables de croire que celle-ci a contrevenu à l'une des dispositions des sections 1 ou 1.1 ou n'a pas mis en œuvre une recommandation énoncée dans l'annexe 1 [18-19] 	<ul style="list-style-type: none"> Le CPVP peut, sur préavis suffisant et à toute heure convenable, procéder à la vérification des pratiques de l'organisation en matière de gestion des renseignements personnels, s'il a des motifs raisonnables de croire qu'elle a contrevenu, contrevient ou est susceptible de contrevenir à la partie 1 de la LPVPC (obligations des organisations) [97-99] 	<ul style="list-style-type: none"> La CAI peut, par une demande péremptoire notifiée par tout mode approprié, exiger de toute personne qu'elle dépose, dans un délai précisé dans la demande, tout renseignement ou de tout document permettant de vérifier l'application de la loi [81.3] Cela s'applique également aux entreprises [83.1] 	<ul style="list-style-type: none"> Le CIPVP de l'Alberta peut mener une enquête pour s'assurer que toute disposition de la PIPA de l'Alberta est respectée [36(1)a)] 	<ul style="list-style-type: none"> Le CIPVP de la C.-B. peut, qu'une plainte soit reçue ou non, entreprendre des enquêtes et des vérifications afin de s'assurer que les dispositions de la PIPA de la C.-B. sont respectées, si le commissaire est convaincu qu'il existe des motifs raisonnables de croire qu'une organisation ne s'y conforme pas [36(1)a); 38; 41(2)(3)] 	<ul style="list-style-type: none"> Chaque autorité de contrôle peut, sous la forme de vérification de la protection des données, mener des enquêtes [58]
25. Conservation des renseignements	<ul style="list-style-type: none"> Pendant le temps nécessaire pour permettre au demandeur d'épuiser tous les recours qu'il a en vertu de la loi [8(8)] Maintenir les renseignements personnels aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés [Ann. 1 – 4.6] 	<ul style="list-style-type: none"> Que le temps nécessaire pour réaliser les fins auxquelles ils ont été recueillis, utilisés ou communiqués ou pour respecter les exigences des lois applicables [53(1)] Pour établir la durée de la période de conservation, l'organisation doit tenir compte de la mesure dans 	<ul style="list-style-type: none"> Aussi longtemps que nécessaire pour satisfaire aux fins prévues [23] Si une demande d'accès ou de rectification est refusée : aussi longtemps que nécessaire pour satisfaire aux fins auxquelles les renseignements personnels ont été recueillis ou utilisés, ou 	<ul style="list-style-type: none"> Aussi longtemps que l'organisation a raisonnablement besoin des renseignements personnels à des fins juridiques ou commerciales [35(1)] L'organisation doit alors a) détruire les dossiers 	<ul style="list-style-type: none"> Obligation pour l'organisation de détruire ses dossiers contenant des renseignements personnels, ou supprimer les moyens par lesquels les renseignements personnels peuvent être associés à des 	<ul style="list-style-type: none"> Pendant aussi longtemps que nécessaire, mais en se limitant au strict minimum [r. 39] Les relevés d'activités de traitement sont requis, sauf pour une organisation employant moins de 250 personnes, sous

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
		<p>laquelle les renseignements personnels sont de nature sensible [53(2)]</p> <ul style="list-style-type: none"> L'organisation qui utilise des renseignements personnels pour prendre une décision concernant un individu conserve ces renseignements suffisamment longtemps pour permettre à l'individu de présenter une demande d'accès [54; 63; 69] Le temps nécessaire pour permettre au demandeur d'épuiser tous les recours qu'il a en vertu de la LPVPC [63; 69] À la demande de l'individu, l'organisation doit procéder au retrait des renseignements personnels le concernant (sauf exception) [55] Veiller à ce que les renseignements personnels soient aussi exacts, à jour et complets que l'exige la réalisation des fins auxquelles ils ont été recueillis, utilisés ou communiqués [56] 	<p>pour permettre à la personne concernée d'épuiser les recours prévus par la loi [36]</p> <ul style="list-style-type: none"> Veiller à ce que tous les renseignements personnels détenus sur autrui soient à jour et exacts lorsqu'utilisés par une entreprise pour prendre une décision relative à la personne concernée Les renseignements utilisés pour prendre une telle décision sont conservés pendant au moins un an suivant la décision [11] Les organisations doivent prévoir un encadrement applicable à la conservation et à la destruction des renseignements personnels dans leurs politiques et pratiques de gouvernance [3.2] 	<p>contenant les renseignements personnels ou b) rendre les renseignements personnels non identifiables, afin qu'ils ne puissent plus être utilisés pour identifier une personne [35(2)]</p>	<p>personnes en particulier, dès qu'il est raisonnable de supposer que a) les fins pour lesquelles ces renseignements personnels ont été recueillis ne sont plus servies par leur conservation et b) la conservation n'est plus nécessaire à des fins juridiques ou commerciales [35]</p> <ul style="list-style-type: none"> Si une organisation utilise les renseignements personnels d'une personne pour prendre une décision qui la concerne directement, elle doit les conserver pendant au moins un an [35] 	<p>réserve de certaines conditions [30]</p>
26. Sanctions prévues par la loi	<p><u>Sanctions pécuniaires</u></p> <ul style="list-style-type: none"> s. o. 	<p><u>Sanctions pécuniaires</u></p> <ul style="list-style-type: none"> Sur recommandation du CPVP, le Tribunal peut infliger des sanctions allant jusqu'à : <ul style="list-style-type: none"> une amende de 10 millions de dollars ou, s'il est supérieur, d'un montant égal à 3 % des recettes annuelles globales 	<p><u>Sanctions administratives pécuniaires</u></p> <ul style="list-style-type: none"> Une personne désignée par la CAI peut imposer des sanctions administratives en cas de non-respect des dispositions de la loi [comme décrit à 	<p><u>Sanctions pécuniaires</u></p> <ul style="list-style-type: none"> s. o. 	<p><u>Sanctions pécuniaires</u></p> <ul style="list-style-type: none"> s. o. 	<p><u>Amendes pécuniaires administratives</u></p> <ul style="list-style-type: none"> Une autorité de contrôle peut infliger des amendes administratives, selon la nature de l'infraction : <ul style="list-style-type: none"> pouvant aller jusqu'à 10 millions d'euros ou 2 %

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
	brutes de l'organisation au cours de son exercice précédant celui pendant lequel elle a été condamnée [95]	l'article 90.1], pouvant aller jusqu'à : <ul style="list-style-type: none"> - 50 000 \$ si le contrevenant est une personne physique - 10 millions de dollars ou le montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé, dans les autres cas [90.12] <ul style="list-style-type: none"> • Possibilité d'éviter une sanction en prenant un engagement auprès de la CAI [90.1] • Le montant de la sanction est déterminé selon différents facteurs [90.2] • Aucune sanction administrative ne peut être imposée à une personne si un constat d'infraction lui a déjà été signifié pour les mêmes raisons [90.11] 			du chiffre d'affaires mondial; ou <ul style="list-style-type: none"> - pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial, selon le plus élevé des deux montants [83]
<p><u>Dispositions pénales</u></p> <ul style="list-style-type: none"> • Lorsqu'une organisation contrevient sciemment aux dispositions énoncées à l'article 28, elle encourt une amende : <ul style="list-style-type: none"> - pouvant aller jusqu'à 100 000 \$ par mise en accusation; ou 	<p><u>Dispositions pénales</u></p> <ul style="list-style-type: none"> • Lorsqu'une organisation contrevient sciemment aux dispositions énoncées à l'article 128, elle encourt une amende : <ul style="list-style-type: none"> - pouvant aller jusqu'à 25 millions de dollars ou, s'il est supérieur, un montant égal à 5 % des recettes globales brutes 	<p><u>Dispositions pénales</u></p> <ul style="list-style-type: none"> • Quiconque contrevient à l'article 91 est passible d'une amende : <ul style="list-style-type: none"> - pouvant aller jusqu'à 100 000 \$, si le contrevenant est une personne physique; ou - pouvant aller jusqu'à 25 millions de dollars ou un 	<p><u>Dispositions pénales</u></p> <ul style="list-style-type: none"> • Quiconque contrevient à l'article 56 est passible d'une amende : <ul style="list-style-type: none"> - pouvant aller jusqu'à 10 000 \$, si le contrevenant est une personne physique; et 	<p><u>Dispositions pénales</u></p> <ul style="list-style-type: none"> • Quiconque contrevient à l'article 59 est passible d'une amende : <ul style="list-style-type: none"> - pouvant aller jusqu'à 10 000 \$, si le contrevenant est une personne physique; et 	<p><u>Dispositions pénales</u></p> <ul style="list-style-type: none"> • Les États membres fixent les règles relatives aux autres sanctions applicables aux infractions au présent RGPD, en particulier pour les infractions qui ne sont pas passibles d'amendes administratives [84]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
	- pouvant aller jusqu'à 10 000 \$ (procédure sommaire) [28]	de l'organisation au cours de l'exercice précédant celui pendant lequel elle a été condamnée; ou - pouvant aller jusqu'à 20 millions de dollars ou, s'il est supérieur, un montant égal à 4 % des recettes globales brutes de l'organisation au cours de l'exercice précédant celui pendant lequel elle a été condamnée [128]	montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice précédent si ce dernier montant est plus élevé, dans tous les autres cas [91] • Les amendes en cas de récidive sont portées au double [92.1] • La sanction est déterminée selon différents facteurs [92.3]	- pouvant aller jusqu'à 100 000 \$, dans tous les autres cas [59(2)]	- pouvant aller jusqu'à 100 000 \$, dans tous les autres cas [56]	
27. Recours auprès de l'organisme de réglementation	• Recours possibles auprès du CPVP [12]	• Recours possibles auprès du CPVP [82] • Ordonnances du CPVP [93] • Recours possibles auprès des tribunaux [inclut 104; 105; 106]	• Recours possibles auprès de la CAI [81] • Ordonnances de la CAI [83]	• Ordonnances du CIPVP de l'Alberta sur l'achèvement d'une enquête [52]	• Ordonnances du CIPVP de la C.-B. sur l'achèvement d'une enquête [52]	• Recours possibles auprès de l'autorité de contrôle compétente [77]
28. Droit d'action privé	• Après avoir reçu le rapport du CPVP ou l'avis l'informant de la fin de l'examen de la plainte, le plaignant peut faire une demande auprès de la Cour en vue d'obtenir des dommages-intérêts (y compris par voie d'une action collective) [14-16]	• Lorsque le commissaire ou le tribunal conclut qu'une organisation a contrevenu à la LPVPC, l'individu touché a une cause d'action en dommages-intérêts, contre cette organisation, pour la perte ou le préjudice résultant de la contravention [107]	• Une personne peut demander directement à un tribunal civil des dommages-intérêts pour perte ou préjudice résultant d'une infraction à la loi (y compris par voie d'une action collective) [<i>Code civil du Québec</i>] • Lorsque l'atteinte est intentionnelle ou résulte d'une faute lourde, le tribunal accorde des dommages-intérêts punitifs d'au moins 1 000 \$ [93.1]	• Lorsque le CIPVP de l'Alberta rend une ordonnance définitive, une personne peut faire une demande à un tribunal en vue d'obtenir des dommages-intérêts pour perte ou dommage résultant d'une violation de la PIPA de l'Alberta [60]	• Lorsque le CIPVP de la C.-B. rend une ordonnance définitive, une personne peut faire une demande en vue d'obtenir des dommages-intérêts pour le préjudice réel résultant d'une violation de la PIPA de la C.-B. [57]	• Toute personne qui a subi un dommage matériel ou non matériel en raison d'une violation du RGPD a le droit de recevoir une indemnisation de la part du responsable de traitement ou du sous-traitant pour le dommage subi (y compris au moyen d'une action collective) [82]

Tableau comparatif des lois pour la protection des renseignements personnels (Canada)

	<i>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)¹</i>	<i>Loi sur la protection de la vie privée des consommateurs (LPVPC), telle que proposée dans le projet de loi C-27²</i>	<i>Loi sur la protection des renseignements personnels dans le secteur privé, telle qu'amendée par le projet de loi 64³</i>	<i>Personal Information Protection Act de l'Alberta (PIPA de l'Alberta)</i>	<i>Personal Information Protection Act de la Colombie-Britannique (PIPA de la C.-B.)</i>	<i>Règlement général sur la protection des données (RGPD)</i>
29. Programmes légaux de certification	<ul style="list-style-type: none"> • s. o. 	<ul style="list-style-type: none"> • Bien qu'elle demeure assujettie à ses obligations en vertu de la LPVPC [80], une organisation peut demander l'approbation du CPVP pour : <ul style="list-style-type: none"> - un <u>code de pratique</u> : prévoit une protection des renseignements personnels équivalente ou supérieure à tout ou partie de celle prévue sous le régime de la LPVPC [76] - un <u>programme de certification</u> : un programme qui répond aux critères énoncés dans le règlement (à venir) [77] 	<ul style="list-style-type: none"> • s. o. 	<ul style="list-style-type: none"> • s. o. 	<ul style="list-style-type: none"> • s. o. 	<ul style="list-style-type: none"> • Les codes de conduite ou les mécanismes de certification pour faciliter le contrôle de la confidentialité [40 à 43]