Comparison between the PPCDA (Bill C-36) and Québec's Private Sector Act

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Enforcement		
Enforcement	Compliance and enforcement of the new act would be done by a new regulator, the Digital Safety and Data Protection Commission of Canada (s. 2(1)).	Provincial regulator, the *Commission d'accès à l'information*, has the power to oversee compliance and enforcement of the Act.
Penalties	Penalties may be imposed for specific contraventions (s. 113). The maximum penalty is the greater of $10,000,000 or 3% of the organization's gross global revenue (s. 114). Certain offences when done knowingly by an organization may lead to such an organization being found either: • Guilty of an indictable offence and liable to a fine not exceeding the greater of $25 million and 5% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced; or • Guilty of an offence punishable on summary conviction and liable to a fine not exceeding the greater of $20 million and 4% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced (s. 145).	AMPs may be imposed on organizations contravening the law. The maximum amount is the greater of $10,000,000 or 2% of worldwide turnover (s. 90.12). Penalties may be imposed for specific offences (s. 91). The maximum amount is the greater of $25,000,000 or 4% of the organization's worldwide turnover.

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Punitive damages	No punitive damages can be awarded.	Individuals can claim punitive damages of at least $1,000 when an unlawful infringement of a right causes an injury, provided the infringement is intentional or results from gross negligence (s. 93.1).
Private right of action	In specific circumstances, the PPCDA grants individuals, affected by an act or omission by an organization that constitutes a contravention of this Act, a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the contravention (s. 132).	The Act also allows for a private right of action in the event of an unlawful infringement of a right conferred by the Act or the Civil Code that causes an injury, and the infringement is intentional or results from a gross fault (s. 93.1).
Consent		
Validity	The PPCDA provides that for consent to be valid, the following information must be disclosed to the individual: • Purposes of collection, use or disclosure; • Manner in which the information is collected, used or disclosed; • Any reasonably foreseeable consequences of collection, use or disclosure of personal information; • The specific types of personal information; and • Third parties to whom the personal information will be disclosed (s. 15(3)).	Similar to Bill C-36, the Act provides that for consent to be valid, certain information must be disclosed to the individual, such as: • Purposes of collection, use or disclosure; • Manner of which the information is collected, used or disclosed; and • Third parties to whom the personal information will be disclosed. However, the Act also requires the disclosure of the following information, which is not the case under the PPCDA: • Rights of access and rectification; • Rights to withdraw consent; • Third parties for whom the personal information is collected, used or disclosed; and • The possibility that personal information might be transferred outside of Québec. Both the reasonably foreseeable consequences of collection, use or disclosure of personal information, and the specific types of personal information, are not required under the Act.

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Format	Consent must be express unless it is appropriate to rely on an individual's implied consent, taking into account the reasonable expectations and the sensitivity of personal information of the personal information that is to be collected, used or disclosed (s. 15(5)). It is not appropriate to rely on implied consent if the individual's personal information is collected or used for a business activity, or collected for legitimate interest (s. 15(6)).	Consent may be implied if the individual, having received the required information, provides their personal information (s. 8.3) Consent should be clear, free and informed. It should be given for specific purposes (s. 14).
Exceptions – Business activities	An organization may collect or use an individual's personal information without their knowledge or consent if: • the collection or use is made for the purpose of a business activity; and • a reasonable person would expect the collection or use for such an activity: the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions (s. 18(1)). The following activities are business activities: • an activity that is necessary to provide a product or service that the individual has requested from the organization; • an activity that is necessary for the security of the organization's information, systems or networks; • an activity that is necessary for the safety of a product or service that the organization provides; and • any other prescribed activity (s. 18(2)).	Under the Act, this exception does not exist.

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Appropriate purposes		
Criterion and factors	Personal information may only be collected, used or disclosed in a manner and for purposes that a reasonable person would consider appropriate in the circumstances (s. 12(1)). All relevant factors must be taken into account in determining whether the manner or purposes are appropriate, including, if appropriate: • the sensitivity of personal information; • whether the purposes represent legitimate business needs of the organization; • the degree of effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs; • whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and • whether the individual's loss of privacy is proportionate to the benefits in light of the measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual (s. 12(2)).	The notion of appropriate purposes is not as detailed or engrained in the Act. However, the Act provides that personal information should be collected for a serious and legitimate reason (s. 4).
Documentation	The organization must determine at or before the time of the collection of any personal information each of the purposes for which the information is or is to be collected, used or disclosed and record those purposes (s. 12(3)). If the organization determines that the personal information it has collected is to be used or disclosed for a new purpose, the organization must record that new purpose before using or disclosing that information for the new purpose (s. 12(4)).	Although not as explicit, the Act provides that the purposes of the collection, use and disclosure of personal information are to be (i) determined prior the collection and (ii) disclosed, and therefore documented, to individuals prior or at the time of the collection (s. 4 and 8).

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Necessity	Only personal information that is necessary for the purposes previously determined may be collected (s. 14(1)).	The Act includes the same requirement as the PPCDA.
Secondary purposes	Use of personal information for purposes other than those determined is not permitted unless the organization obtains the individual's valid consent before any use or disclosure for that other purpose (s. 14(1). Consent is not required for those secondary purposes where certain exemptions apply (such as business activities, anonymization or de-identification, etc.) (s. 14(2)).	The Act includes the same requirement as the PPCDA.
Governance		
Fundamental right	Privacy is recognized under the PPCDA as a fundamental right (s. 5).	There is no equivalent provision in the Act.
Control – Accountability	Organizations are accountable for personal information that is under their control (s. 7(1)). Information is considered under an organization's control when the organization decides to collect the information and determines the purposes for its collection, use or disclosure, regardless the information is collected, used or disclosed by the organization itself or by a service provider on behalf of the organization (s. 7(2)).	The Act includes a similar requirement; under the Act, organizations are responsible for personal information they hold (s. 3.1).
Privacy officer	An organization must designate one or more individuals to be responsible for matters related to its obligations under the legislation. It must provide the designated individual's business contact information to any person who requests it (s. 8(1)).	The requirement under the Act is slightly different. The designated official is automatically the person with the highest authority, unless the responsibility is delegated. The contact information should be published on organizations' websites and provided on demand (s. 3.1).

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Privacy management program	Organizations must implement a privacy management program, including policies, practices and procedures respecting: • the protection of personal information, • how requests for information and complaints are received and dealt with; • training procedures provided to the organization's staff respecting its policies, practices and procedures; and • the development of materials to explain the organization's policies and procedures (s. 9(1)). The privacy management program must take into account the volume and sensitivity of personal information (s. 9(2)).	Policies must: • provide a framework for the keeping and destruction of the information; • define the roles and responsibilities of the organization and its personnel throughout the life cycle of the information; and • provide a process for dealing with complaints regarding the protection of the information. The policies and practices must also be proportionate to the nature and scope of the enterprise's activities, approved by the person in charge of the protection of personal information, and approved by the Privacy Officer (s. 3.2).
Transparency	An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfill its obligations, including : • a description of the type of personal information under the organization's control; • a general account of how the organization uses personal information and of how it applies the exceptions to the requirement to obtain an individual's consent under this Act, including a description of any activities in which it has a legitimate interest; • a general account of the organization's use of any automated decision system (see below); • whether or not the organization transfers or discloses personal information across provinces or outside of Canada that may have reasonably foreseeable privacy implications (see below); • the retention periods applicable to sensitive personal information; • how an individual may make a request for disposal or access; and • the business contact information of the individual to whom complaints or requests for information may be made (s. 62).	The requirement is not as detailed under the Act, but it is required to publish detailed information about those policies and practices (listed above), in simple and clear language on the organization's website or, if the organization does not have a website, made available by any other appropriate means (s. 3.2 (2)).

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Anonymization and De-identification		
Definitions	Information is "anonymized" if it is modified irreversibly and permanently so there is no reasonably foreseeable risk in the circumstances that an individual can be identified from the information, whether directly or indirectly, by any means. Information is "de-identified" when the personal information is modified so that an individual cannot be directly identified from it, although a risk of the individual being identified remains (s. 2(1)).	Information is anonymized if it is, at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly (s. 23 para. 2) Information is "de-identified," under the Act, if it no longer allows the person concerned to be directly identified (s. 12).
Anonymization	Bill C-36 explicitly establishes that the legislation does not apply to anonymized information (s. 5(4)). It also provides that an organization may use an individual's personal information without their knowledge or consent to either de-identified or anonymized personal information (s. 20).	No equivalent provision. The Act only provides that anonymization should be carried out in accordance with best practices and the terms provided for in the *Regulation respecting the anonymization of personal information*, RLRQ, c. A-2.1, r. 0.1.
De-Identification	In addition to section 20, Bill C-36 provides that organizations that de-identify personal information must: • consider, when applying technical and administrative measures to the information, the risk of an individual being identified; and • ensure that those measures are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information (s. 74). However, an organization is prohibited from using de-identified personal information, alone or in combination with other information to identify an individual, except: • to conduct testing of the effectiveness of security safeguards that it has put in place; • in circumstances where the personal information was de-identified solely for the purpose of protecting the information;	There is no equivalent provision in the Act and its regulations.

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
De-Identification ***(continued)***	• in circumstances where the organization obtains the individual's valid consent; • in circumstances where there is an exception in respect to the use of an individual's personal information (only applicable in certain instances); • in circumstances where the personal information is used solely for the purpose of anonymizing it; • to comply with any requirements under this Act or under federal or provincial law; • to conduct testing of the fairness and accuracy of models, processes and systems that were developed using de-identified personal information; • to conduct testing of the effectiveness of its de-identification processes; • for a purpose or situation authorized by the Division; and • in any other prescribed circumstances. If an organization knowingly contravenes section 75, it may be found either: • Guilty of an indictable offence and liable to a fine not exceeding the greater of $25 million and 5% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced; or • Guilty of an offence punishable on summary conviction and liable to a fine not exceeding the greater of $20 million and 4% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced (s. 145).	

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Artificial Intelligence		
Definition	"Automated decision system" is defined as any technology that assists or replaces the judgment of human decision-makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network, or another technique.	There is no equivalent definition.
Accuracy	An organization must take reasonable steps to ensure that personal information under its control is as accurate, up to date and complete as is necessary to fulfill the purposes for which the information is collected, used or disclosed (s. 55(1)). As part of its analysis to determine to which extent personal information must be accurate, complete and up to date, the organization must take into account the individual's interest; and • whether the information may be used to make a decision about the individual; • whether the information is used on an ongoing basis; and • whether the information is disclosed to third parties. Routine updating is not required unless it is necessary to fulfill the purposes for which the information is collected, used or disclosed (s. 55).	Although there is a requirement for personal information to be accurate and up to date (s. 11), the Act does not contain any requirements on the extent to which the information must be accurate.
Governance	• Organizations are required to make readily available, in plain language, information that explains organizations' practices and policies, including, without limitation, a general account of their use of automated decision-making to make predictions, recommendations or decisions about individuals that could have a legal or similarly significant effect on them (s. 62(2)(c)).	There is no equivalent requirement in the Act.

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Transparency	Upon request of an individual, if the organization has used an automated decision system to make predictions, recommendations or decisions about the individual that could have a legal or similarly significant effect on them, the organization must provide an explanation. Such an explanation must include the following elements: • reasons or principal factors that led to the prediction, recommendation or decision; • the type of personal information used to make the prediction, recommendation or decision; and • the source of the information. Organizations must also provide individuals with the opportunity to submit written representations to an employee who is able to review the prediction, recommendation or decision (s. 63(4) to (6)).	Contrary to the PPCDA, organizations that use personal information to render a decision based exclusively on an automated processing of such information must inform individuals of the use of such systems, at the latest, at the time they inform the individual of the decision (s. 12.1). Upon request, organizations must also provide: • reasons, factors and parameters that led to the decision • personal information used to render the decision; and • the right of the individual concerned to have the personal information used to render the decision corrected. Organizations must provide individuals with the opportunity to submit observations to a member of the personnel of the enterprise who is in a position to review the decision (s. 12.1).
Outsourcing & cross-border transfers		
Outsourcing agreement	Transfer to service providers is possible without the individual's consent (s. 19). Prior to doing so, organizations must ensure, by contract or otherwise, that the service provider provides a level of protection in respect to the personal information equivalent to that which the organization is required to provide under the legislation (s. 11(1)).	Similar to Bill C-36, it is possible to transfer personal information to service providers or have them collect personal information on the organization's behalf, without the individual's consent, if a written agreement is concluded (s. 18.3). Contrary to Bill C-36, the agreement must include a certain number of provisions, such as: • physical, organizational and technical measures to be put in place by the service providers; • obligation to only use the information for the purposes of the service to be provided by the service provider; • obligation to destroy the information after the expiration of the contract; • obligation to notify the organization in case of attempted or actual confidentiality incidents; and • possibility for organizations to conduct audits of the service provider's safety and confidentiality practices (s. 18.3).

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Governance	The PPCDA provides that the obligations provided for organizations, with the exception of some, do not apply to a service provider in respect to personal information that is transferred to it. However, the service provider is subject to all of the obligations that apply to organizations, if it collects, uses or discloses that information for any purpose other than the purposes for which the information was transferred to it (s. 11(2)).	There is no equivalent provision under the Act.
Cross-border transfers	Before an organization communicates or transfers personal information outside Canada, the organization must: • conduct a privacy impact assessment (PIA); and • implement measures to mitigate the identified risks, such as contractual measures and adherence to code of practice or a certification process (s. 57(1)).	A PIA must be conducted prior to the transfer outside of the province and not just outside of the country as stated in the PPCDA (s. 17). The PIA must take into account: • the sensitivity of the information; • the purposes for which it is to be used; • the protection measures that would apply to it, including those that are contractual; and • the legal framework applicable in the State in which the information would be communicated, including the personal information protection principles applicable in that State. The information must only be transferred if the protection provided is adequate. Measures must be implemented to mitigate the risks identified in the PIA, and a written agreement must be made and contain the results of the PIA, including the mitigating measures (s. 17).
Transparency	As mentioned above, information on the possibility of transfers of personal information across provinces or outside of Canada that may have reasonably foreseeable privacy implications must be disclosed (s. 62(2)(d)).	Similarly to the PPCDA, the possibility of personal information being transferred outside of the province of Québec must be disclosed to individuals. However, it cannot be disclosed as general information on the organization's policies, but rather to the individual prior to the collection of personal information (s. 8).

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Breach of safeguards	If a service provider determines that any breach of security safeguards has occurred that involves personal information, it must notify the organization that controls the personal information as soon as feasible (s. 61).	The Act provides for a similar requirement.
Safeguards and incident response		
Safeguards	Organizations must protect personal information through physical, organizational and technological security safeguards. The level of protection provided by those safeguards must be proportionate to the sensitivity of the information. In addition to the sensitivity of the information, the organization must, in establishing its security safeguards, take into account: • the quantity of the information; • the distribution of the information; • the format of the information; • the method of storage of the information, and • any reasonably foreseeable privacy implications that may arise in relation to the transfer of personal information to a service provider (s. 56 (1) and (2)). Security safeguards must protect personal information against, among other things, loss, theft or unauthorized access, disclosure, copying, and use or modification, and must include reasonable measures to authenticate the identity of the individual to whom the personal information relates (s. 56(3)). For the purpose of Bill C-36, "breach of security safeguards" means the loss of unauthorized access to, or unauthorized disclosure of, personal information resulting from a breach of an organization's security safeguards that are referred to in section 56 or from a failure to establish those safeguards (s. 2(1)).	The factors to take into account for the implementation of security measures are slightly different than the ones listed in the PPCDA. Under the Act, safety measures must be applied considering: • the sensitivity; • purposes; • quantity; and • distribution of personal information.

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Notification	A breach must be reported to the Commission and the individual if there is a real risk of significant harm. "Significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property (s. 58(7)). The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include: • the sensitivity of the personal information involved in the breach; • the probability that the personal information has been, is being, or will be misused; and • any other prescribed factor (s. 58(8)).	A breach must be reported to the Commission and individuals if there is a risk of serious injury. No definition for the risk of serious injury is provided in the Act (Regulation respecting confidentiality incidents, RLRQ, c. A-2.1, r. 3.1).
Register	Organizations must, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control (s. 60(1)). Organizations must, on request, provide the Commission with access to, or a copy of, the record (s. 60(2)). If an organization knowingly contravenes section 60, it may be found either: • Guilty of an indictable offence and liable to a fine not exceeding the greater of $25 million and 5% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced; or • Guilty of an offence punishable on summary conviction and liable to a fine not exceeding the greater of $20 million and 4% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced (s. 145).	There is an equivalent requirement to maintain a register of confidentiality incidents under the Act (Regulation respecting confidentiality incidents, RLRQ, c. A-2.1, r. 3.1).

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Individual rights		
Right to access	Organizations must, on request, inform individuals of: • whether they have any personal information about them; • how they use the information and whether they have disclosed the information; • giving the individual access to the information (s. 63(1)); and • if the organization has disclosed the information, the names of the third parties or types of third parties to which the disclosure was made, including in cases where the disclosure was made without the consent of the individual (s. 63(3)). An organization is not required to act on a request in respect of de-identified personal information (s. 63(2)). Requests are to be made by individuals in writing (s. 64(1)). Organization must provide the information in plain language or in an alternative format to an individual with a sensory disability who requires that it be transmitted in that format, if : • A version of the information already exists in that format; or • Its conversion into that format is reasonable and necessary in order for the individual to be able to exercise their rights under the legislation (s. 66(2)). For medical information, an organization may choose to give the individual the information through a medical practitioner (s. 66(3)). Organizations must respond in 30 days to the request, subject to extensions (s. 67). If an organization fails to respond to the request within the time limit, the organization is deemed to have refused the request (s. 67(4)).	Similarly to the PPCDA, organizations must, on request: • confirm the existence of personal information; • communicate the information to the individual and allow him to obtain a copy of it. Requests for access must also be made in writing. Specific to the Act, computerized personal information must be communicated in the form of a written and intelligible transcript (s. 27 para. 2) and, similarly to Bill C-36, if the individual is handicapped, reasonable accommodation must be provided on request to enable the individual to exercise the right of access (s. 27 para. 4). The Act includes the same delay to respond to a request (30 days), but does not allow for a time extension. It also does not include that medical information may be communicated to the individual via a medical practitioner. Access is free unless fees of charge, but a reasonable charge may be required from an individual that requests the transcription, reproduction and transmission of personal information (s. 33). Similarly to Bill C-36, prior to requiring a charge, the organization must inform the individual in advance of the approximate amount that will be charged (s. 33). When refusing a request, the organization must provide the reasons in writing and inform the individual of a possible recourse within 30 days of receiving the request (s. 34).

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Right to access ***(continued)***	Access is free, unless: • The organization has informed the individual of the approximate cost; • The cost to the individual is minimal; and • The individual has advised the organization that the request is not being withdrawn (s. 68). When refusing a request, the organization must provide the reasons in writing and inform the individual of a possible recourse within 30 days of receiving the request (s. 67(3)).	
Right to rectification	If an individual has been given access to their personal information and demonstrates that the information is: • inaccurate; • incomplete; or • outdated. The organization must amend the information as required (s. 71). This requirement will not apply to de-identified information (s. 71(2)) and organizations must, if it is appropriate, transmit the amended information to any third party that has access to the information (s. 71(3)). If the organization and the individual do not agree on the amendments that are to be made to the information, the organization must record the disagreement and, if it is appropriate to do so, inform third parties that have access to the information of the fact that there is a disagreement (s. 71(4)).	An individual may request rectification if the data is: • inaccurate; • incomplete; • equivocal; or • unlawfully collected, communicated or retained. There are no similar requirements when it comes to de-identified information, the obligation to transmit amended information to the third-party service providers, and the disagreements. In addition, the right to rectification under the Act is not conditioned on the individual having been granted access, as it currently appears to be the case in the PPCDA.

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Right to de-indexation	Bill C-36 does not include this right.	Under certain conditions and upon request, organizations must cease disseminating personal information or de-index any hyperlink attached to individuals' names that provides access to the information (s. 28.1).
Right to data portability	On the request of an individual, an organization must, as soon as feasible, disclose the personal information that it has collected from the individual to an organization designated by the individual, if both organizations are subject to a data mobility framework (s. 72).	The right to data portability is more detailed in the Act. Under the Act, unless doing so raises serious practical difficulties, organizations required to disclose computerized personal information collected from an individual, and not created or inferred using personal information concerning him, must, at his request, be communicated to him in a structured, commonly used technological format. The information must also be communicated, at the applicant's request, to any person or body authorized by law to collect such information (s. 27 para. 3).
Right to deletion	Upon request, organizations are required to dispose of the individual's personal information as soon as feasible under three circumstances: • the information was collected, used or disclosed in contravention of this Act; • the individual has withdrawn their consent; or • the information is no longer necessary. It is important to note that the definition of the term "dispose" under Bill C-36 includes the act of anonymizing personal information in addition to its deletion (see the section below for more information).	There is no explicit right to delete personal information under the Act. The right to have personal information is an extension of the right to rectify personal information only.

Topic	**PPCDA (Bill C-36)** *Protecting Privacy and Consumer Data Act*	**Québec's Private Sector Act** *Act respecting the protection of personal information in the private sector*
Retention and disposal		
Retention	Organizations must not retain personal information for a period longer than necessary to: • fulfill the purposes for which the information was collected, used or disclosed; or • comply with the requirements of this legislation, of federal or provincial law, or of the reasonable terms of a contract. Retention periods for sensitive information must be disclosed to the individual, as part of the transparency requirements listed above (s. 62).	The requirement for retention of personal information is equivalent under the Act. However, there is no obligation to disclose retention periods for sensitive personal information.
Disposal	The definition of the term "dispose" includes not only the permanent and irreversible deletion of personal information, but also the act of anonymizing personal information (s. 2(1)). Organizations must dispose of the information as soon as feasible after the periods listed above (s. 52(1)).	The requirements are similar under the Act as personal information must also be destroyed or anonymized once the purpose is achieved (s. 23).
Third-party providers	Organizations that received a request for disposal of an individual must, as soon as feasible, inform any service provider to which it has transferred the information of the request, and ensure that the service provider disposes of the information (s. 54(5)).	Service providers are required to destroy personal information they have obtained once the services have been provided, and the contract expires or is terminated (s. 18.3).

Authors

Élisabeth Lesage-Bigras
T 514.395.2749
ELesageBigras@blg.com

Krystin Chung
T 416.367.6000
KChung@blg.com

Candice Hévin
T 514.954.2588
CHevin@blg.com

Frédéric Wilson
T 514.954.2509
FWilson@blg.com

Key contacts

Hélène Deschamps-Marquis
T 514.954.3102
HDeschampsMarquis@blg.com

Dan Michaluk
T 416.367.6097
DMichaluk@blg.com

Frédéric Wilson
T 514.954.2509
FWilson@blg.com

Eric Charleston
T 416.367.6566
ECharleston@blg.com

Borden Ladner Gervais