Borden Ladner Gervais

Canada's *Protecting Privacy and Consumer Data Act* (Bill C-36):

What businesses need to know

June 2026

On June 15, 2026, the Minister of Artificial Intelligence and Digital Innovation, Evan Solomon, introduced Bill C-36, *An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts*.

This long-awaited piece of legislation is the faithful successor of the former Bill C-27, which died on the order paper in January 2025. Bill C-36 introduces the *Protecting Privacy and Consumer Data Act* (PPCDA), which replaces the privacy provisions found in the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The PPCDA follows the federal government's release of AI for All: Canada's National Artificial Intelligence Strategy (AI for All), whose first pillar, "Protecting Canadians and safeguarding democracy," emphasizes that public trust in AI requires modern privacy and online safety laws, strong national AI safety capabilities, and secure government systems, such as with the Safe Social Media Act (Bill C-34). In line with the AI federal strategy, the PPCDA represents a modernized and stronger privacy and data protection legal framework in Canada.

In terms of scope, the PPCDA remains essentially aligned with PIPEDA: it applies to the collection, use and disclosure of personal information by an organization in the course of commercial activities, as well as to employee personal information in respect of federal works, undertakings or businesses. It is also intended to apply across Canada, except in provinces that have enacted substantially similar private-sector privacy legislation.[1]

BLG prepared this guide to explain the proposed PPCDA, provide practical information for organizations, and give comparative insights with current privacy regimes in Canada and overseas.

This document will be updated as the bill goes through the legislative process.

Last updated: June 23, 2026

[1] Note that section 139 allows the Governor in Council to exempt an organization or activities, as well as categories of organizations or activities, from the application of the PPCDA, provided that a substantially similar law is applicable in the province of the organization or activities. For the purpose of this exemption, the Governor in Council can make regulations to establish factors and processes that will determine if a provincial law is sufficiently similar.

Table of contents

What you need to know

- Bill C-36 is currently at the initial stage of the legislative process, having completed the first reading of the House of Commons on June 15, 2026. As of this date, there is no clear sense of when it may be enacted and come into force.

A new enforcement paradigm

- A new regulatory body, the Digital Safety and Data Protection Commission of Canada, is proposed to replace the Office of the Privacy Commissioner
- Administrative penalties of up to the greater of $10 million and 3 per cent of global revenue
- Fines for certain offences, up to the greater of $25 million and 5 per cent of global revenue (for indictable offences) or $20 million and 4 per cent of global revenue (for summary conviction offences)
- A new private right of action allowing individuals to seek damages for contraventions of the PPCDA in certain circumstances
- Codes of practice and certification programs as a new voluntary compliance tool

New Individual rights, new operational challenges

- Three new individual rights: the right to be informed of automated decision-making, the right to disposal, and the right to mobility

Heightened accountability and governance obligations

- Clarification that personal information is controlled by the organization that collects it and determines the purposes for its collection, use and disclosure
- A new obligation to establish, implement and make available a privacy management program
- Establishing the role and responsibilities of service providers

Consent made easier (or not)?

- By default, consent must be obtained expressly, unless implied consent is suitable
- New consent exceptions for de-identified information and legitimate business practices

A pro-AI stance

- Definitions and new requirements for de-identification and anonymization practices
- A carve-out from most individual rights for de-identified information
- A new consent exception for internal research, analysis and development when information is de-identified
- New transparency requirements for automated-decision making

1. Enforcement

1.1 New Commissioner (s.76)

The Office of the Privacy Commissioner of Canada (OPC) would no longer be in charge of overseeing the federal private sector privacy regime. Instead, it is being replaced by the new Digital Safety and Data Protection Commission of Canada (the Commission), also established under the *Digital Safety Act* (Bill C-34). The Commission consists of five members appointed by the Governor in Council, one of whom is designated the Privacy and Consumer Data Commissioner (the Commissioner).

With this major change, Bill C-36 centralizes federal privacy enforcement within a single regulator in charge of digital-related enforcement at large. This model differs from Québec, the European Union and the United Kingdom, where privacy enforcement is carried out by commissioners in charge of data protection.

It also departs from the approach proposed in Bill C-27, which would have created a separate tribunal to impose administrative monetary penalties. Under Bill C-36, the new Commission has the powers to impose administrative monetary penalties, subject to review and appeal mechanisms before the Federal Court.

Appointment. The appointment model for the new Commissioner also marks an important institutional shift. Under the current framework, the Privacy Commissioner of Canada is an agent of Parliament, appointed with the approval of both the House of Commons and the Senate, and reporting directly to Parliament. This model is intended to reinforce the Commissioner's independence from the government.

Bill C-36 provides for the Commissioner to be appointed by the Governor in Council (in practice, the cabinet) instead, which may raise questions about the institutional independence of the new regulator, particularly given its expanded enforcement powers and broader digital regulatory mandate.

Losing a pragmatic and trusted regulatory voice. Over time, the OPC has developed a level of practical expertise that goes beyond a traditional enforcement role. In particular, it has built a meaningful advisory capacity for private-sector organizations, supported by experienced resources and a strong understanding of operational realities.

In addition, the OPC also plays an active role in international privacy forums, including the Global Privacy Enforcement Network and the G7 data protection authorities' roundtable. These engagements support alignment with global trends and enhance the OPC's ability to address cross-border issues.

In a data economy where enforcement increasingly involves multinational organizations, global vendors and cross-border data flows, this international experience may also support greater consistency in the interpretation and application of Canadian privacy law. The transition towards a new regulator therefore carries a real risk that this accumulated expertise, developed over time through practice, engagement and international cooperation, will be difficult to replicate within a newly established regulatory framework.

Current powers maintained. The PPCDA carries forward certain powers found in PIPEDA, including that individuals may file complaints and that the Commissioner can initiate a complaint on its own initiative. The Commissioner also maintains the following powers:

- Carrying out investigations in respect of a complaint;
- Entering into compliance agreements with organizations who have contravened the statute; and
- Conducting audits regarding an organization's compliance with the statute.

The PPCDA would also maintain the OPC's authority to issue guidance materials and provide advisory services to organizations upon request.

New powers. The PPCDA also grants the Commissioner significant new powers to issue compliance orders if it is deemed reasonably necessary to ensure compliance with the Act. The compliance orders may force contravening organizations to:

- Take necessary measures to comply with the statute;
- Stop doing something that contravenes the statute;
- Comply with a compliance agreement; and
- Make public any measures to correct its policies, practices or procedures.

It is also interesting to note that both the Commission and Commissioner must consider the best interests of children, as well as the importance of supporting economic growth, competition and innovation in the Canadian marketplace when exercising their powers.

1.2 Monetary penalties (ss. 113, 145)

As part of the notice of contravention, the Commissioner is also required to decide whether to impose a penalty, similar to privacy regulators under other regimes, such as the GDPR and Québec's *Act respecting the protection of personal information in the private sector* (Private Sector Act).[2]

Contraventions. Penalties of up to the greater of $10,000,000 and 3 per cent of the organization's gross global revenue may be imposed for contraventions in relation to:

- Implementing an adequate privacy management program;
- Transferring personal information to a service provider;
- Ensuring personal information is collected, used and disclosed according to appropriate purposes;
- Limiting collection, use and disclosure of personal information;
- Obtaining consent for a new purpose;
- Obtaining valid consent;
- Explaining the consequences of withdrawing consent;
- Retaining personal information for necessary periods only;
- Disposing of personal information at an individual's request;
- Ensuring service providers dispose of personal information if personal information was transferred;
- Protecting personal information through security safeguards;
- Reporting security breaches to the Commission and the individual;
- Service providers notifying the organization in case of a breach; and
- Making policies and procedures readily available and in plain language.

[2] See article 58(2)(i) of the GDPR and article 90.1 of the Québec Private Sector Act.

Offences. For indictable offences, penalties of up to the greater of $25,000,000 or 5 per cent of the organization's gross global revenue may be imposed, or for offences punishable on summary conviction, penalties of up to the greater of $20,000,000 or 4 per cent of the organization's gross global revenue, if the organization knowingly:

- Does not report a security breach to the Commission;
- Does not keep records of security breaches;
- Does not retain personal information for a sufficient amount of time in the context of an access request;
- Uses de-identified information in prohibited circumstances;
- Contravenes an order of the Commission following a notice of contravention;
- Disadvantages a whistleblower.

1.4 Appeals (ss. 126-128)

The PPCDA grants complainants and organizations a right to appeal to the Federal Court any decision issued by the Commissioner in which it finds that the organization has contravened, or not contravened, the PPCDA. Applications must be made within 30 days following the issuance of the decision.

1.5 Private right of action (s.132)

The PPCDA introduces a new private right of action.

Individuals affected by a contravention of the PPCDA may bring a claim against the organization for damages to compensate for loss or injury suffered due to that contravention, provided that: (a) the Commissioner has found that the organization contravened the PPCDA and that finding is final; (b) the Federal Court has found that the organization contravened the PPCDA; (c) a final decision dismissing any appeal or confirming the contravention has been made and all rights of appeal exhausted; or (d) the Commissioner has entered into a compliance agreement with the organization

The PPCDA also provides individuals with a private right of action against the organization convicted of an offence under section 145 of the PPCDA.

In each case, the private right of action must be acted upon in the two years after an individual becomes aware of the date of the Commissioner's finding, review decision, or appeal decision.

Unlike Québec's Private Sector Act, which provides for statutory damages under section 93.1 in certain circumstances, the PPCDA does not create a statutory damages regime, which likely means that the risk of privacy class actions introduced in the Federal Court would remain marginal compared to what is currently being witnessed in Québec.

1.6 Whistleblowing and anti-reprisal provisions (ss. 143-144)

The PPCDA maintains the whistleblowing protection that is currently included in PIPEDA. The Commissioner has used information received under this provision to initiate a complaint on at least one occasion (PIPEDA Case Summary #310). The PPCDA also includes an anti-reprisal provision that mirrors the one included in PIPEDA.

1.7 Codes of practice and certification programs (ss. 92-96)

The PPCDA provides for the creation of "codes of practice" and "certification programs," a means of encouraging voluntary, sectoral practices that favour privacy protection. Similar provisions are included in Articles 40 to 43 of the GDPR and may provide for greater certainty in the application of the PPCDA.

In order to further encourage the development of improved and consistent privacy practices, the PPCDA will allow any organization, whether or not subject to the PPCDA or government institutions, to seek the Commissioner's approval of codes of practice and certification programs. The organization may choose to voluntarily comply and maintain certification as a means of both reducing the risks associated with non-compliance with the PPCDA and highlighting its commitment to privacy compliance. However, doing so will not necessarily be proof of full compliance with the PPCDA.

Penalties for contraventions of the PPCDA are not to be imposed if the organization, at the time of contravention, was in compliance with the requirements of a certification program approved by the Commission. This safe harbour underscores the value of approved codes of practice as a strategic compliance mechanism for organizations.

2. Accountability and governance

The PPCDA codifies and elaborates on the Principle of Accountability currently articulated in Schedule 1 of PIPEDA. While the changes to current requirements appear relatively limited, some notable additions under the PPCDA will likely enhance the clarity of those requirements for businesses.

2.1 Notion of control (s.7)

As under PIPEDA, the PPCDA provides that an organization is accountable for personal information under its control. The PPCDA goes further by stating that personal information "is under the control of the organization that decides to collect it and that determines the purposes for its collection, use or disclosure." The PPCDA is clear that an organization has control over personal information even when the organization transfers the information to a service provider, or where the information is collected, used or disclosed by a service provider on behalf of the organization.

Similar to the GDPR, the PPCDA distinguishes the obligations applicable to the controlling organization and service providers, the latter not being subject to Part I of PPCDA (which addresses the obligations of the organization), except for security safeguards and notification to customers in case of a breach.

2.2 Role of the privacy officer (s.8)

Under the PPCDA, the organization must designate an individual to be responsible for the organization's obligations under the Act, a role typically referred to as the "privacy officer." The organization must also provide the designated individual's business contact information to any person who requests it. The PPCDA does not specify who within the organization must fulfill this role.

2.3 Privacy management program (s.9)

The PPCDA will require each organization to implement and maintain a privacy management program that includes the policies, practices and procedures the organization implements to fulfill its PPCDA obligations.

The required subject matter of these policies is generally the same as under PIPEDA: they must address the protection of personal information, the handling of inquiries and complaints, the training of staff on policies and procedures, and the development of materials to explain the policies and procedures.

Notably, the PPCDA introduces a new requirement that an organization, when developing its privacy management program, consider the volume and sensitivity of the personal information under its control. This is likely intended to reinforce the Commissioner's long-standing message that the organization's policies and safeguards need to be reasonable with regard to the types of information it handles.

The PPCDA will also require that an organization give the Commissioner access to its policies, practices and procedures upon request. Although PIPEDA does not contain an equivalent requirement, the organization will generally provide such materials to the OPC in any event. The key change is that the PPCDA adds that, after reviewing such materials, the Commissioner may provide guidance, or recommend that corrective measures be taken.

2.4 Record of purposes (s.12)

Additionally, the PPCDA requires an organization to identify and record each of the purposes for which it collects, uses or discloses any personal information, at or before the time of collection. If the organization determines that the personal information 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.

Currently, PIPEDA relies on a more flexible, principles-based obligation to identify and document purposes without mandating a comprehensive data inventory. With this requirement, the PPCDA is brought closer to the GDPR's recording requirement under Article 30, which requires a formal, structured record of processing activities.

In practice, this requirement could reveal itself to be burdensome for organizations collecting personal information for a myriad of purposes, seeing how best practices require that a proper register of logs be maintained.

3. Consent

The PPCDA makes significant changes to the notion of consent by introducing a consent exception for specified business activities, as well as a more flexible exception for certain processing operations carried out for the purpose of an activity in which the organization has a "legitimate interest."

In doing so, the PPCDA moves away from the often-criticized consent-centric model favoured by the current federal legislative regime to a more balanced approach that recognizes that consent is neither realistic nor reasonable in all circumstances. In short, the PPCDA seeks to strike a better balance between the legitimate business interests of the organization in processing personal information and the privacy rights of Canadians.

3.1 Form of consent (s.15)

Express consent is the default form of consent under the PPCDA, but an organization may rely on implied consent if doing so is "appropriate" in the circumstances, having regard to the "reasonable expectations of the individual" and the "sensitivity" of the personal information.

While the former is not explicitly defined in the legislation, the PPCDA adds a new definition for "sensitive information," modelled on the OPC's interpretation bulletin on sensitive information. This definition includes children's personal information, which elevates the standard of consent for this particular type of information. For other types of information, sensitivity will need to be assessed contextually.

It is also interesting to note that, in comparison with how the OPC defined sensitive information in its interpretation bulletin,[3] the PPCDA's definition does not include financial data, a clear indication that the legislature intends to preserve a contextual approach to the type of information.

The PPCDA introduces a potentially significant limitation on the notion of implied consent when processing is carried out in accordance with one of the new consent exceptions. In particular, the PPCDA creates a rule by which implied consent is deemed inappropriate if the collection or use of personal information is carried out for an activity falling within the scope of the new consent exception for specified business activities, or for activities in which the organization has a legitimate interest.

These distinctions seem to strengthen the notion of consent by requiring the organization to rely on one of the consent exceptions noted above, or to obtain express consent for one or more of the activities described in those provisions. However, given the breadth of activities potentially covered by the legitimate interest exception (further discussed below in Section 3.4), it is unclear to what extent an organization can rely on implied consent without first undertaking a privacy impact assessment (PIA) in accordance with section 18(4)(b) PPCDA (as discussed in more detail below).

We can expect the scope and application of section 15(6) PPCDA to be clarified as C-36 progresses through the legislative process.

[3] "Information that will generally be considered sensitive and require a higher degree of protection includes health and financial data, ethnic and racial origins, political opinions, genetic data, neural data, uniquely identifying biometric data, an individual's sex life or sexual orientation, and religious or philosophical beliefs."

3.2 Privacy notice and informed consent (s.15)

Information to provide. Regardless of the form of consent, an organization must provide the individual whose consent is sought with certain types of information to ensure that their consent is sufficiently informed. The PPCDA requires the following elements to be provided at or before the time consent is sought:

- Purposes for which personal information is processed;
- Manner in which personal information is processed;
- Any reasonably foreseeable consequences resulting from the processing operations;
- Specific type of personal information that is to be processed; and
- Names of any third parties or types of third parties to which the personal information may be disclosed

These requirements closely reflect the OPC's Guidelines for obtaining meaningful consent, but appear to go further than Québec's consent guidance, particularly through the express requirement to disclose any reasonably foreseeable consequences resulting from the processing. The scope of this requirement will need to be clarified, including whether it extends to behavioural consequences or influence-related effects, especially given the federal government's broader policy objective of addressing data-driven surveillance practices, as addressed in its AI for All strategy.

Format. The PPCDA now clarifies that the information described above needs not only be provided in "plain language," but in a language that is also sufficiently adapted to the target audience, such that it would be reasonable to expect them to "understand" the content of the notice. This is substantially in line with the requirement found under section 6.1 PIPEDA.

A key challenge that remains largely unresolved by C-36 is the actual manner and format in which this notice must be presented to an individual. For example, tools often used by the organization to present content in a convenient and accessible manner, such as layered and just-in-time notices, are not explicitly mentioned, despite the OPC's recommendation to use such mechanisms in its interpretation bulletin. While still lacking clear rules on format, content structure and accessibility of information, the organization must nevertheless consider the potential challenges resulting from the overall context in which consent is being sought when determining how to furnish or actively direct individuals to relevant information.

Deceptive practices. Section 16 further strengthens the PPCDA's consent framework by providing that an organization must not obtain, or attempt to obtain, an individual's consent by providing false or misleading information, or by using deceptive or misleading practices, and that any consent obtained in those circumstances is invalid.

Such practices are not explicitly defined in the Act. However, Bill C-36 uses language that closely aligns with the OPC's 2024 Sweep Report on deceptive design patterns, which describes such patterns as design choices used on websites and apps to influence, manipulate or coerce users into decisions that are not in their best interests, and that may prevent them from making informed choices about the collection, use and disclosure of their personal information. It also borrows from a broader consumer protection vocabulary from the *Competition Act* and consumer protection laws.[4] It will be interesting to follow how such a provision is interpreted in regard to consent flows and cookie banners.

[4] For e.g.: s. 219 of Québec's *Consumer Protection Act*, chapter P-40.1.

3.3 Withdrawal of consent and other key requirements (s.15)

The PPCDA largely maintains the status quo with respect to some of the other key consent-related requirements of PIPEDA. For example, consent to processing operations that are not necessary for the provision of a product or service cannot be a condition of service (optionality of consent); an individual is entitled to withdraw consent at any time, subject to reasonable notice and applicable law or the reasonable terms of a contract (withdrawal of consent); and consent remains invalid if it was obtained by providing false or misleading information, or using deceptive or misleading practices (consent obtained by deception).

3.4 New consent exceptions (ss. 18, 20-22)

Most consent exceptions found under PIPEDA are carried over to the PPCDA, with limited changes. The PPCDA introduces a number of new consent exceptions, including for certain specific business activities, and a more flexible exception in which an organization has a legitimate interest that "outweighs any potential adverse effect on the individual" resulting from the collection or use of their personal information.

These exceptions, as well as a few others introduced for de-identified personal information, are discussed in more detail below.

Specified business activity exception. An organization may collect or use personal information without the individual's knowledge or consent if such processing is carried out for the purpose of a specified business activity, other than influencing the individual's behaviour or decisions (which arguably includes advertising and marketing), and falls within an individual's reasonable expectations.

In particular, the PPCDA specifies that the following activities qualify as "business activities":

- The provision of a product or service that the individual has requested from the organization;
- The organization's information, system or network security;
- The safety of a product or service that the organization provides; and
- Any other activity prescribed by regulation.

The exclusion for activities carried out for the purpose of influencing an individual's behaviour or decisions may prove particularly important in the context of advertising, website cookies and similar tracking technologies.

Because the purpose of advertising could arguably be said to influence an individual's decisions, one could argue that organizations should not be able to rely on that exception for cookies used for behavioural advertising, personalization, retargeting, or other influence-oriented purposes. In practical terms, this hypothesis would mean that express consent will likely remain required for advertising (and online, for many non-essential cookies), even where the organization might otherwise argue that the activity supports its business operations, and falls within the individual's reasonable expectations.

A similar exclusion is also included for the collection of electronic addresses by use of computer programs designed or marketed primarily for use in generating, searching for, or collecting electronic addresses. Such activities will require explicit consent from individuals.

Legitimate interest exception. A significant development is the inclusion of a new, flexible legitimate interest exception for collecting or using personal information without the individual's knowledge or consent. In particular, an organization may rely on this exception where personal information is collected, used or

disclosed for the purpose of an activity in which (i) the organization has a legitimate interest that outweighs any reasonably foreseeable adverse effect on the individual resulting from the collection, use or disclosure; (ii) the personal information is not collected, used or disclosed for the purpose of influencing the individual's behaviour or decisions; and (iii) such processing falls within an individual's reasonable expectations.

In line with the privacy regulator's calls for greater authority in using personal information to be accompanied by greater accountability for organizations, an organization must, prior to relying on this exception:

- Identify the legitimate interest;
- Conduct and record a PIA and, on request, provide a copy of the assessment to the federal privacy commissioner;
- Identify reasonable measures implemented to reduce the likelihood that the effects will occur, or to mitigate or eliminate them; and
- Demonstrate compliance with any other requirements prescribed by regulation.

While an organization that relies on this exception can collect and use personal information without an individual's knowledge and consent, it bears noting that an organization must nevertheless be transparent in its privacy policy about how it applies consent exceptions, including by providing a description of any activities falling within the scope of the legitimate interest exception.

Although similar to the GDPR's notion of legitimate interest, the PPCDA's legitimate interest exception is just that, an exception to the notion of consent, not an alternative and separate legal basis for processing data on an equal footing with consent. However, unlike the GDPR, this exception does not explicitly permit consideration of the legitimate interest of another person (that is, other than that of the organization collecting or using the information).

It is not clear at this stage what specific types of activities might or might not fall within an organization's "legitimate interest" and, in particular, whether this might extend to product improvement, the development of new products or services, or even certain forms of advertising or marketing, such as direct marketing or location-based advertising.

Publicly available information. Under the PPCDA, information that is publicly available and which is specified by regulations can be collected, used or disclosed without requiring consent. This new exception might open the door to debates about its interpretation, similar to *Clearview AI Inc v Alberta (Information and Privacy Commissioner)*, 2025 ABKB 287.

Disclosure to lawyer or notary. Like under PIPEDA, the PPCDA allows an organization to disclose personal information without consent to a lawyer or notary. By contrast, Québec's Private Sector Act takes a broader approach.[5] While it generally requires a written agreement when personal information is communicated to a service provider, it exempts members of professional orders from the requirement to specify, in that agreement, the measures that must be taken to protect the personal information. As a result, under the PPCDA, disclosures to members of a professional order other than lawyers or notaries would still require appropriate contractual protections, whereas Québec law would exempt such professionals from the prescribed content requirements for third-party agreements.

[5] See article 18.3.

Specific exceptions for de-identified personal information. In addition to permitting the use of personal information without knowledge or consent for de-identification, the PPCDA offers the organization the following consent exceptions for de-identified information:

- **Internal research, analysis and development exception.** An organization may use de-identified information for its internal research, analysis and development purposes (s.21 PPCDA). This represents a broad permission, and one that may incentivize organizations to de-identify personal information in order to enable broader internal use, including for commercially valuable activities.
- **Prospective business transaction.** While the PPCDA requires parties to a prospective business transaction to de-identify personal information (among other requirements) in order to use or disclose such information without the individual's knowledge and consent, this requirement has been tempered.

  In particular, the organization is not required to de-identify the information prior to use or disclosure if doing so would undermine the objectives of carrying out the transaction, and the organization has taken into account the risk of harm resulting from such processing. For example, during the due diligence phase of a transaction, it is necessary to know the identity of specific individuals, such as individuals in decision-making or strategic positions, or key employees, including for public searches, conflict-of-interest screening or background checks.

  These requirements point to the need for specific contractual protections at the letter of intent stage, in addition to the ones respecting use, protection, and return or destruction of information received prior to the closing of a transaction. In practice, without the exception, the requirement will prove difficult to comply with where transaction deadlines are often short, and sellers are frequently smaller companies with fewer resources.

3.5 Appropriate purposes (s. 12)

PIPEDA includes a catchall reasonableness test (that is, the "reasonable person" test), which dictates the limits of its application, and which may apply even if consent was obtained from individuals. The PPCDA includes a similar requirement under which an organization may collect, use or disclose personal information only in a manner and for purposes that a reasonable person would consider appropriate in the circumstances.

While this provision of the PPCDA under C-36 is similar to the one provided under PIPEDA, the wording "in a manner" was added in C-36, and the new bill also specifies that this reasonableness test applies "whether or not consent is required under this Act."

The PPCDA provides the factors that must be taken into account in determining whether the manner and the purposes are appropriate. These factors are largely the same as those elaborated in the *Turner v. Telus Communications Inc.* decision in which the Federal Court, and subsequently the Federal Court of Appeal, set out the factors for evaluating whether an organization's purpose is in compliance with subsection 5(3).[6] These factors are:

- The sensitivity of the personal information;
- Whether the purposes represent legitimate business needs of the organization;
- The 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.

As discussed above (see Record of purposes), under the PPCDA, at or before the time of the collection of personal information, each of the purposes for which the information is to be collected, used or disclosed must be determined and recorded.

[6] See also OPC's Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), May 2018.

4. Individual rights

The PPCDA formally recognizes privacy as a "fundamental right."

As with PIPEDA, the PPCDA grants individuals the right to access and rectify their personal information. The PPCDA also provides individuals with new rights relating to automated decision-making, data deletion, and data mobility under specified circumstances. Interestingly, the PPCDA expressly excludes personal information that has been de-identified from some – but not all – of the individual rights set out in the PPCDA.

4.1 Right to access and amendment (ss. 63-71)

Right to access. As with PIPEDA, the PPCDA gives individuals the right to find out what personal information an organization holds about them and to access it.

On written request, an organization must inform the individual in plain language:

- Whether it holds any personal information about them;
- How it uses that information; and
- Whether it has disclosed that information – and if so, the names or types of third parties involved, including disclosures made without consent.

It must also give the individual access to the information itself. PIPEDA allows an organization to provide an individual with a list of third parties to which it may have disclosed the individual's personal information if it is not possible to provide an accurate list of third parties to which disclosure was made, an option that is notably absent from the PPCDA.

Right to amendment. As with PIPEDA, the PPCDA gives individuals the right to have their personal information rectified. The organization must amend information that the individual shows is inaccurate, outdated or incomplete. Where appropriate, the organization must also pass the amended information to any third party that has access to it.

If the organization disagrees with the requested amendments, it must keep a record of the disagreement and, where appropriate, inform any third parties with access to the information about it.

It is interesting to note that the right to amendment seems to be tied to the right to access, as section 71(1) PPCDA conditions the right to amendment to the individual first being given access to their personal information. This would be a departure from PIPEDA, under which the right to rectification existed as a standalone right. However, it is unlikely that the legislature intended to limit requests for correction to situations where the access right has been formally exercised, as an individual who believes an organization holds inaccurate information could reasonably rely on section 55 PPCDA (accuracy of information) and the organization's general obligation to ensure that personal information is accurate.

4.2 Right to data mobility (ss. 72, 140)

The PPCDA innovates in section 72 by creating a limited right to data portability, which will allow individuals to request that an organization discloses to a third-party organization designated by the individual, as soon as feasible, information that the first organization has collected from the individual, provided that both organizations are subject to a "data mobility framework." Importantly, the mobility right extends only to personal information that the organization collects from individuals (which is to say, not from third parties).

Data mobility frameworks. The PPCDA allows the Governor in Council to make regulations that:

- Set the safeguards the organization must have in place for the secure disclosure and collection of personal information, and the technical parameters needed to ensure interoperability between systems;
- Specify which organizations are subject to a data mobility framework; or
- Create exceptions to the disclosure requirement, including to protect proprietary or confidential commercial information

The PPCDA's mobility right is narrower than that of Québec's Private Sector Act and the GDPR, as both these portability rights apply generally, without comparable restrictions on which organizations may be subject to data mobility requests. As a result, the PPCDA does not fully open the door to permit the general portability requests found in each of Québec's Private Sector Act and the GDPR.

Although subject to different rules, the recently enacted *Consumer-Driven Banking Act* (Bill C-15) can be seen as a sector-specific application of this broader right to data mobility. Together, both data mobility regimes contribute to the federal government's goal of allowing better data flows between organizations for the sake of consumers, as expressed in the 2025 federal budget.

4.3 Right to disposal (s.54)

The PPCDA gives individuals a new right to request that an organization dispose of their personal information. To dispose means to permanently and irreversibly delete personal information or to anonymize it. However, the PPCDA's right to disposal does not include a right to de-indexation, or a right to be forgotten, unlike in Québec's Private Sector Act and the GDPR.

The organization must comply, as soon as feasible, if:

- The information was collected, used or disclosed in contravention of the PPCDA;
- The individual has withdrawn consent; or
- The information is no longer necessary for a product or service the individual requested.

While some may argue that a similar obligation already existed implicitly under PIPEDA where consent was withdrawn, or the original purposes had been completed, the PPCDA goes further. In particular, the right to disposal may apply even where a broader purpose has not necessarily been exhausted, if the information is no longer necessary for the product or service requested by the individual.

For example, where an organization collected personal information both to provide a service and for secondary purposes such as marketing, an individual who no longer wishes to benefit from the service may be able to request disposal even though the organization might previously have argued under PIPEDA that it could retain the information for other recorded purposes.

Significantly, if the personal information targeted by the request was transferred to a service provider, the PPCDA requires organizations to inform them as soon as feasible, and ensure the disposal is enforced. This requirement will be burdensome and difficult to implement for organizations dealing with many service providers.

For the last two grounds only (that is, withdrawal of consent and the information no longer being necessary), the organization can refuse if:

- The information can't be severed from another individual's personal information without undue burden;
- Another law or contract prevents disposal;
- The information is needed for a legal defence or remedy;
- Disposal would harm the accuracy or integrity of information needed for an ongoing product or service where the information doesn't relate to a child;
- The request is vexatious or made in bad faith; or
- The adverse effect of disposal on the organization outweighs the adverse effect of retention on the individual.

A refusal must be explained in writing, including the individual's options to challenge it under the PPCDA. If the refusal is based on the "adverse effect to the organization" ground, it must also be reported to the Commission. And if the data was shared with a service provider, the organization must make sure that provider deletes it too.

A caveat: De-identified information and individual rights

The PPCDA excludes de-identified personal information from the rights to access and rectification, data mobility, and disposal – a carve-out that appears to acknowledge the commercial burden the organization would otherwise face in re-identifying information to comply with those rights. In practice, this creates a strong incentive for the organization to de-identify personal information before using it for research and development, rather than seeking consent to use the information in its native state.

5. Artificial intelligence and automated decision systems

By introducing provisions on de-identification and anonymization, the PPCDA provides long-anticipated provisions adapted to the current era of artificial intelligence. Recent federal policy signals, including the government's AI for All strategy, make clear that Canada intends to address many AI-related risks, including those relating to fairness, safety, democratic integrity, deepfakes, algorithmic bias, online harms, and the misuse of personal information through a safety-first approach grounded in law. Against this backdrop, the PPCDA's AI-related provisions reflect the continuation of a broader policy direction: using privacy and data protection law as a primary instrument to govern the development and deployment of AI systems, including by strengthening safeguards against inappropriate uses of personal information and emerging practices such as surveillance-based pricing.

The PPCDA finally clarifies the distinction between "anonymize" and "de-identify," which allows for greater predictability. Importantly, the PPCDA allows the organization to de-identify or anonymize personal information without the individual's knowledge or consent, resolving a long-standing ambiguity under PIPEDA.

5.1 Anonymization (ss.2(1), 6(5), 20, 54)

Under the PPCDA, "anonymize" means to irreversibly and permanently modify personal information so that there is no "reasonably foreseeable risk" that an individual can be directly or indirectly identified from it. The PPCDA does not apply to anonymized personal information, and anonymization is also considered a form of disposal.

This inclusion of a reasonableness standard in the assessment of re-identification risk is also consistent with Québec's own anonymization regime (see section 23 of the Private Sector Act and the *Regulation respecting the anonymization of personal information*), which similarly frames anonymization by reference to whether re-identification risk is reasonably foreseeable.

For organizations, a clear legal framework governing the use of anonymized information is important to support innovation, product development and the training of AI models, while providing greater certainty as to when information falls outside the scope of the PPCDA. The Act accordingly provides that anonymization of personal information may be subject to prescribed regulations (s. 139 (1) (a) PPCDA).

No consent required. While the definition of anonymization confirms that it involves modifying personal information, section 20 PPCDA clarifies that organizations may "use" personal information and apply anonymization techniques to it without the individual's knowledge or consent.

This is significant in practice: organizations do not need to anticipate anonymization uses at the time of collection or include those purposes into their privacy notices, which provides important flexibility to leverage data for secondary purposes such as analytics, research or product improvement once it has been properly anonymized.

Although Québec law does not contain an explicit, equivalent provision, the same conclusion should generally apply under Québec's *Regulation respecting the anonymization of personal information*, since information that has been anonymized in accordance with the applicable standard should no longer be treated as personal information, and therefore should not trigger consent requirements.

5.2 De-identification (ss. 2(1), 2(2), 20-22, 54(3))

"De-identify" means to modify personal information so that an individual cannot be directly identified from it, although a risk of identification remains. Unlike anonymized information, de-identified information does not cease to be personal information. However, it is exempt from the PPCDA's disposal obligations, as well as access- and amendment-related obligations.

The PPCDA establishes rules for handling de-identified personal information and creates specific exceptions allowing its use or disclosure without an individual's consent. This allows the organization to benefit from greater flexibility with respect to processing such de-identified information.

Handling de-identified information (ss. 74-75, 145). The relatively undemanding threshold chosen for de-identification – the removal of directly identifying information – makes it possible for the organization to preserve the richness of record-level data essential for internal research. However, the PPCDA imposes specific obligations when handling de-identified information: the organization must consider the risk of an individual being identified when applying technical and administrative measures, and ensure those measures are proportionate to the purpose and the sensitivity of that information.

The PPCDA prohibits the organization from using de-identified personal information, alone or in combination with other information, to identify an individual, except:

- To test the security safeguards or de-identification processes that it has put in place;
- Where the personal information was de-identified solely to protect it, or to anonymize it;
- With the individual's valid consent;
- To test the fairness and accuracy of models, processes and systems developed using de-identified personal information;
- To comply with the PPCDA or other federal or provincial law;
- As authorized by the Privacy and Consumer Data Division, or in any other prescribed circumstances; or
- Where another PPCDA provision applies.

Under the PPCDA, the organization that knowingly contravenes the prohibition would be liable to a fine of up to the higher of $25,000,000 or five per cent of the organization's gross global revenue. Together, the prohibition and this penalty implicitly recognize the inherent risk of re-identification associated with de-identified data, and aim to balance its use against the protections and restrictions needed to minimize that risk.

Consent exceptions for de-identified information (ss. 21, 22). The PPCDA permits the organization to use and, in some cases, disclose, personal information without an individual's knowledge or consent if it is de-identified, including:

- For internal research, analysis and development purposes, provided the information is de-identified before use; and
- Between parties to a prospective business transaction, provided the information is de-identified before use or disclosure and remains so until the transaction is completed.

- The PPCDA thereby permits the organization to reuse information collected for one purpose for secondary research purposes, such as enterprise or business analytics. The prohibition provision regarding de-identified information also confirms what had been anticipated with respect to machine learning: using de-identified information to train machine learning systems would arguably also fall within the "research and development" exception.

Exception - Re-identification (s.75). The PPCDA creates an exception to the general prohibition on re-identifying individuals using de-identified personal information, permitting the organization to test the fairness and accuracy of models and systems developed using de-identified information. The reference to "models" is almost certainly meant to refer to the output of a machine learning process: the trained result is routinely referred to as a "model" in AI literature.

As a result, the organization testing machine learning models for fairness, accuracy or bias would not be impeded by re-identification restrictions, even where the underlying training data was de-identified.

5.3 Automated decision systems

"Automated decision system" means, under the PPCDA, any technology that assists or replaces human judgment in decision-making, including rules-based systems, regression analysis, predictive analytics, machine learning, deep learning, neural networks, or other techniques.

The proposed definition of "automated decision system" is deliberately broad and technology-neutral. It captures not only AI-based tools, but also more traditional rules-based systems that are widely used across organizations. Importantly, the definition is not limited to technologies that fully replace human decision-making. It also extends to systems that merely support or inform human judgment.

In practice, and by comparison with section 12.1 of Québec's Private Sector Act, which applies only to decisions based exclusively on automated processing, this significantly expands the scope of captured systems, as many operational tools are designed to structure, guide or influence decisions rather than automate them entirely. Under the PPCDA, the definition of personal information expressly captures information inferred about an individual – extending to AI-generated inference.

Openness and transparency (s. 62). The organization using an automated decision system must make readily available, in plain language, a general account of how the system is used to make predictions, recommendations, or decisions about individuals that could have a legal or similarly significant effect on them.

While the phrase "legal or similarly significant effect" is neither defined nor elucidated, legal effects could be interpreted in practice as decisions impacting an individual's rights and obligations. As for "similarly significant effect," one natural interpretation may draw on the circumstances that give rise to "significant harm" as defined under the PPCDA, such as damages to reputation, loss of employment, financial loss, or negative effects on an individual's credit record.

Under the EU, guidance has been published on the interpretation of the terms "legal or similarly significant effect." For example, France's Commission Nationale de l'Informatique et des Libertés wrote that such effect would mean that an individual's environment, behaviour or choices are influenced, or that the result would be discriminatory. Whereas the UK's Information Commissioner Office does not define such a criterion, it gives the examples of "automatic refusal of an online credit application, and e-recruiting practices without human intervention" as having similarly significant effects.

In contrast with section 12.1 of Québec's Private Sector Act, the PPCDA captures not only decisions, but also predictions and recommendations, provided they could have a legal or similarly significant effect on the individual. For organizations, the inclusion of this threshold is a welcome limitation and appears to be borrowed from Article 22 of the GDPR,[7] which refers to a decision based solely on automated processing, including profiling, that produces legal effects concerning the data subject, or similarly significantly affects them.

This breadth creates a key operational challenge: organizations will need to identify and inventory all in-scope systems, which may prove complex in practice. Many tools with decision-shaping functionality are embedded in business processes, and not always formally categorized as "automated decision systems," requiring a more granular and cross-functional mapping exercise.

Right to be informed of automated decision-making (s.63(5)). The PPCDA gives individuals a new right to request an explanation of automated decisions, recommendations, or predictions that could have a legal or similarly significant effect on them. This right is reflected in the GDPR, but has no equivalent under PIPEDA. On request, the organization must explain:

- The personal information used;
- The source of that information; and
- The principal reasons for the outcome

Individuals must also be given an opportunity to make written representations to an employee who can review the outcome, and organizations must assist individuals that would need any assistance in preparing such written representations.

The content of the explanation, although similar, goes further than section 12.1 Québec's Private Sector Act, by requesting the sources of the information. Unlike the GDPR, however, the PPCDA does not give individuals the right to object to the use of automated decision-making. Moreover, it is unclear whether the right to rectification extends to conclusions reached by an automated decision system.

[7] See Article 22 of the GDPR: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

6. Children

The PPCDA introduces an explicit definition of "child," which effectively replaces the generally favoured use of the term "minor." The Act defines a "child" as an individual under 18 years of age.

A key feature of the PPCDA is that personal information relating to children is deemed to be sensitive. This is significant because sensitivity is not confined to one provision of the Act; it is a recurring factor that informs the organization's obligations across the privacy lifecycle. As a result, any organization that collects, uses or discloses children's personal information should conduct a more cautious assessment of whether its practices are appropriate in the circumstances.

Consent (s. 15(5)). The sensitivity of children's personal information is relevant to consent. Because sensitivity is one of the factors used to determine whether implied consent is appropriate, organizations will often need express consent when collecting and processing children's information.

Appropriate purposes (s. 12(2)). Because the reasonable person test expressly requires consideration of the sensitivity of the information, organizations collecting, using, or disclosing children's information should carefully assess whether the purposes and the manner of collecting, using or disclosing are appropriate.

De-identification (s.74). The PPCDA requires organizations to consider both the purpose and the sensitivity of the information when applying technical and administrative measures to de-identified information. Where children's data is involved, organizations should therefore consider stronger de-identification techniques, stricter access limits, and additional controls to reduce the risk of re-identification or inappropriate secondary use.

Cybersecurity and incident response (ss. 56, 58). The PPCDA's safeguarding obligation is proportionate to the sensitivity of the information, meaning that organizations handling children's personal information should assess whether additional administrative, technical and organizational safeguards are required, including access controls, authentication measures, monitoring, staff training and controls over service providers. Moreover, children's personal information will also be relevant when assessing whether a breach creates a real risk of significant harm.

Retention and disposal (ss. 52, 54(2)). Since the PPCDA requires organizations to take sensitivity into account when determining retention periods, children's personal information should generally be subject to shorter retention periods, with appropriate and careful justification where longer retention is necessary.

The exception allowing an organization to refuse a disposal request if doing so would have an undue adverse effect on the accuracy or integrity of information that is necessary to the ongoing provision of a product or service to the individual does not apply if it concerns a child's personal information.

Authorized representatives (s. 4). The rights provided for under the PPCDA may be exercised on behalf of a child by a parent, guardian or tutor, unless the child (i) wishes to personally exercise those rights, and (ii) is capable of doing so. Unlike in Québec's Privacy Act (that is, 14 years old) or the GDPR (in this case, 13 years old), there is no specific age limit to exercise privacy rights, including the right of recourse.

7. Outsourcing and cross-border

The PPCDA does not materially change outsourcing or cross-border requirements. Rather, it formally incorporates existing requirements and best practices, and clarifies the respective obligations of both an organization with personal information under its control and its service providers. It also confirms the obligations of service providers that use personal information for their own purposes. For businesses, these changes are likely to provide greater clarity and consistency.

7.1 Outsourcing

The PPCDA clarifies how personal information may be transferred to a service provider, which is defined as "an organization, including a parent corporation, subsidiary, affiliate, contractor or subcontractor that provides services for or on behalf of another organization to assist the organization in fulfilling its purposes."

This definition confirms that entities of the same organization are included as service providers. It should be noted that the terms "services for or on behalf of another organization" appear to have a large scope, and are not further defined.

Additionally, the PPCDA introduces new requirements for the organization that discloses or transfers personal information outside Canada.

Obligations of the organization (ss. 7, 11, 19, 54, 56). Under the PPCDA, the organization may transfer an individual's personal information to a service provider without their knowledge or consent. Québec's Private Sector Act contains an equivalent provision at section 18.3.

As defined under section 7 of the PPCDA, personal information collected, used or disclosed by a service provider on the organization's behalf remains under the control of the organization, not the service provider, so long as the organization decides to collect the information and determines the purposes of its collection, use or disclosure.

The organization must:

- Ensure, by contract or otherwise, that the service provider provides the information with a level of protection equivalent to what the organization itself must provide under the PPCDA;
- Establish its security safeguards and take into account any reasonably foreseeable privacy implications that may arise in relation to the transfer of personal information to a service provider; and
- Inform any service provider to which personal information was transferred as soon as feasible after disposing of that information at an individual's request, and ensure that the service provider also disposes of it.

In practice, this means that the organization, prior to transferring the information to a third party, should enter into a data processing agreement (DPA).

Obligation of service providers (ss. 11, 19, 54(5), 56(2), 61, 71(3)). As opposed to PIPEDA, obligations are expressly imposed on service providers under the PPCDA. Service providers are obligated to establish appropriate security safeguards, and they must notify as soon as feasible the organization in case of a

security breach. Organizations controlling personal information are then in charge of notifying individuals and the Commission. Moreover, service providers must be able to execute a request for amendment or disposal presented to the controlling organization.

In contrast, Québec's Private Sector Act does not contain an exact equivalent provision expressly imposing security-safeguard and breach-notification obligations directly on service providers. Instead, the organization remains responsible for reasonable security measures and breach notification under sections 10 and 3.5, while section 18.3 requires DPAs to include confidentiality protections and restrictions on use. In practice, service-provider security and incident-notification obligations are therefore addressed contractually.

Although the PPCDA more clearly imposes specific obligations on each party, we still recommend that organizations establish roles and responsibilities in case of a breach in a DPA.

Although a service provider is not otherwise bound by Part 1 of the PPCDA for information it processes on another organization's behalf, it becomes subject to all such obligations if it collects, uses or discloses personal information transferred by another organization for any purpose other than the one for which it was transferred.

7.2 Cross-border transfers (ss. 6, 57, 62)

The PPCDA applies to personal information that the organization collects, uses or discloses interprovincially or internationally. Before disclosing or transferring personal information outside Canada, an organization must:

- Complete a PIA and provide the Commission with access to, or a copy of, the PIA on request;
- Implement measures to mitigate the risks identified in the PIA, such as contractual privacy protection measures, adherence to a code of practice, or certification process approved by the Privacy and Consumer Data Division; and
- Disclose whether it transfers or discloses personal information interprovincially or internationally in a manner that may have reasonably foreseeable privacy implications

The new PIA requirement for cross-border transfers brings the PPCDA closer to Québec's framework, where section 17 of the Private Sector Act requires a privacy impact assessment before communicating personal information outside Québec. In practice, the PPCDA formalizes a requirement that was already widely recognized as a best practice for international transfers.

It may also be read as part of a broader federal concern with data sovereignty: Pillar 4 of *AI for All* focuses on building a Canadian sovereign AI foundation, and emphasizes that sovereignty in the AI era depends not only on infrastructure and computing capacity, but also on the data that fuels AI systems.

8. Safeguards and incident response

The PPCDA includes a security-safeguarding obligation very similar to that currently in effect under PIPEDA: an obligation to protect personal information through "proportionate" physical, organizational and technological security safeguards. Sensitivity would become the new primary factor governing the adequacy of security safeguards, though "the quantity, distribution, format and method of storage of the information" would continue to be relevant.

An organization can benchmark whether its security safeguards are "proportionate" by conducting a structured, risk-based assessment that aligns the sensitivity and volume of personal information it holds with the likelihood and impact of harm from a breach, and then comparing its controls against recognized standards (such as NIST CSF or ISO 27001), regulatory guidance, and peer practices in its sector.

This typically involves documenting identified risks, mapping existing physical, technical and organizational safeguards to those risks, testing their effectiveness (through audits or tabletop exercises), identifying gaps where controls fall short of industry norms for similarly situated organizations, and creating a mitigation plan.

8.1 Authentication (s.56)

The PPCDA expands the scope of the organization's security-safeguard obligations. In addition to protecting personal information against loss, theft or unauthorized access, disclosure, copying, use, or modification, the organization must also implement reasonable measures to authenticate the identity of the individual to whom the personal information relates.

Notably, the new requirement applies only to "authentication" – verifying or confirming an individual's identity – and not to "identification," which involves searching a database to determine who a person is.

The PPCDA requires the organization to implement security safeguards that are "reasonable" for this verification purpose, rather than for identifying an individual outright. To this end, the organization should weigh the risk of fraud and identity theft when assessing appropriate safeguards for the personal information used in authentication, and should consider adopting information security best practices.

8.2 Notification and reporting (ss. 58-59, 61)

The PPCDA preserves the notification and reporting requirements that apply to "breach of security safeguards" as they exist under PIPEDA, namely by requiring the organization to take the following steps where a breach of security safeguards creates a real risk of significant harm:

- Report the breach to the Commission;
- Notify the affected individual of the breach as soon as feasible after the organization determines that the breach has occurred;
- Notify any other organization or a government institution of the breach if the organization believes that doing so may help reduce or otherwise mitigate the risk of harm.

The PPCDA would also introduce a new requirement for service providers: if a service provider determines that a breach of security safeguards involving personal information has occurred, it must notify the organization that controls the information as soon as feasible.

This would establish a statutory minimum for service provider notification, a matter typically governed by the terms of service provider agreements. The trigger for notification – a determination that a breach of security safeguards involving personal information has occurred – would give the service provider time to investigate security incidents before giving notice. Like PIPEDA and the Québec Privacy Act, there is no fixed delay for notification, which must be given as soon as feasible, without specifying a fixed deadline as under the GDPR (for example, within 72 hours).

9. Retention and disposal

Similar to PIPEDA's Principle 5, the PPCDA imposes duties on the organization regarding information retention. An organization must not retain personal information longer than the period necessary to:

- Fulfill the purposes for which it was collected, used or disclosed; or
- Comply with the PPCDA, other federal or provincial law, or the reasonable terms of a contract.

Once that period ends, the organization must dispose of the information as soon as feasible. Organizations should note that the definition of "dispose" includes anonymization, which could prove useful when destruction would be impractical or difficult.

The PPCDA, however, is more prescriptive than PIPEDA by adding the requirement that, when setting the retention period, the organization must factor in the sensitivity of the information. If the information was used to make a decision about an individual, it must be retained for a sufficient period to allow the individual to make an access request (as a reference, such period is of one year under the Québec Privacy Act). As with PIPEDA, the organization must also retain the information for as long as necessary to allow the individual to exhaust any recourse under the PPCDA.

Next steps

Bill C-36 is currently awaiting second reading at the House of Commons, as the first reading was completed on June 15, 2026. After, the Senate will need to conduct its own three readings before officially adopting the Act. As of June 2026, there is no clear indication of how fast the bill will reach the next steps.

BLG will update this document as the bill progresses through the legislative process to accurately reflect legal changes.

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