The Protecting Privacy and Consumer Data Act (Bill C-36)

Key obligations and enforcement overview

June 2026

OSLER

Table of contents

About Osler's Privacy and Data Management Group

Osler has the largest team of practitioners who focus on privacy and data management in Canada. Our team is comprised of acknowledged leaders in the privacy arena, and our Group is consistently recognized by industry-leading publications, including the only Band 1 ranking in *Chambers Canada* for Privacy and Data Protection.

We provide advice on the increasingly complex rules and the broad range of privacy and data-governance issues arising from the collection, use, disclosure and management of personal information. Our fully integrated team is uniquely positioned to provide a comprehensive service offering that includes high-stakes legal services and innovative online privacy information solutions. We are acknowledged leaders in complex data governance, cybersecurity incident response, and emerging, high-value areas such as data analytics and AI regulation.

Through our innovative AccessPrivacy by Osler thought leadership offering, we provide a series of information products and solutions for Chief Privacy Officers, in-house privacy counsel and privacy compliance professionals. Our offerings include a complimentary Monthly Privacy Call that provides updates on emerging privacy and related developments in the Canadian privacy and data arena, privacy in the courts quarterly updates, and an on-line subscription-based platform. Our monthly call has thousands of subscribers across the private, health and public sectors, and is relied upon by many organizations as a regular part of their privacy awareness.

Contributors

Adam Kardash
Co-Chair and Partner, Privacy and Data Management, Toronto

Éloïse Gratton, Ad. E.
Co-Chair and Partner, Privacy and Data Management, Montréal

Joanna Fine
Partner, Privacy and Data Management, Toronto

John Salloum
Partner, Privacy and Data Management, Toronto

François Joli-Coeur
Partner, Privacy and Data Management, Montréal

Adam LaRoche
Partner, Privacy and Data Management; Employment and Labour, Calgary

Katelyn Smith
Associate, Privacy and Data Management, Toronto

Komil Joshi
Associate, Privacy and Data Management, Toronto

Tina Saban, CIPP/C
Associate, Privacy and Data Management, Toronto

Catherine Hart
Associate, Privacy and Data Management, Toronto

Maryna Polataiko
Associate, Privacy and Data Management, Toronto

Erika Romanow
Associate, Privacy and Data Management, Calgary

Alannah Safnuk
Associate, Privacy and Data Management, Toronto

Naomi Chernos
Associate, Privacy and Data Management, Toronto

Marguerite Rolland
Associate, Privacy and Data Management, Montréal

Alexandra Toma
Associate, Privacy and Data Management, Toronto

Cassandre Legault
Associate, Privacy and Data Management, Montréal

Colleen Morawetz
Privacy Knowledge Management Lawyer, Toronto

Executive summary

On June 15, 2026, the Government of Canada 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* (Bill C-36), in the House of Commons at first reading. If enacted, the *Protecting Privacy and Consumer Data Act* (PPCDA) will repeal Part 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and establish a modernized federal private-sector privacy regime for Canada.

The PPCDA is the third iteration of federal privacy reform legislation following Bill C-11 (2020) and Bill C-27 (2022), both of which died on the order paper. It is substantially similar to the *Consumer Privacy Protection Act* (the CPPA) proposed in Bill C-27 but includes several notable updates, including a new enforcement framework centred on the Digital Safety and Data Protection Commission of Canada.

This overview summarizes the PPCDA and identifies the principal differences between the PPCDA and PIPEDA as well as between the PPCDA and the CPPA.

Status note
This document describes Bill C-36 as introduced at first reading in the House of Commons on June 15, 2026. The legislation may be amended as it proceeds through the parliamentary process. It does not constitute legal advice and should not be relied upon as a substitute for obtaining legal advice specific to your organization's circumstances.

Key themes

The PPCDA retains PIPEDA's consent-based, principles-based, technology-neutral regime grounded in balancing individual privacy rights and organizational interests, while introducing

- a substantially strengthened enforcement regime, with administrative monetary penalties (AMPs) of up to the higher of $10 million or 3% of gross global revenues, penal fines for offences of up to the higher of $25 million or 5%, a private right of action and order-making powers
- a new regulatory model under the Digital Safety and Data Protection Commission of Canada, replacing the Office of the Privacy Commissioner (the OPC)
- clarified and expanded exceptions to consent, including for defined business activities and legitimate interests
- express provisions on de-identified and anonymized information
- a mandatory privacy management program
- codified service provider rules and cross-border transfer requirements, including a new privacy impact assessment obligation before disclosing or transferring personal information outside of Canada
- statutory recognition of codes of practice and certification programs
- new individual rights: disposal (deletion/anonymization) and data mobility
- enhanced protections for children's personal information
- transparency requirements regarding automated decision systems

1

What the PPCDA keeps and what it changes

1.1 Continuity with PIPEDA

The PPCDA preserves fundamental aspects of PIPEDA, including

- a balancing of the interests of individuals and organizations
- a consent-based regime as the primary authority for processing personal information
- rules generally drafted in a principles-based, risk-calibrated, technologically neutral fashion
- an accountability model pursuant to which organizations are responsible for personal information under their control

1.2 Key new features introduced by the PPCDA

The PPCDA introduces a range of new and materially enhanced features, including

- an enforcement regime with potentially severe financial penalties, a private right of action, and order-making power for the regulatory authority
- clarified and expanded exceptions to consent, including for defined business activities and for processing based on legitimate interests (subject to compliance with strict obligations)
- provisions relating to de-identified and anonymized information, with clarification that anonymized information falls outside the application of the PPCDA
- strengthened and more prescriptive accountability requirements, including an obligation to implement a mandatory privacy management program
- clarification of the obligations on service providers

- statutory recognition of codes of practice and certification programs
- new individual rights: a right of disposal (deletion/anonymization) and a right of data mobility
- transparency provisions regarding automated decision systems, including a right to an explanation and written representations

1.3 Key updates from the CPPA (Bill C-27)

Although the PPCDA is substantially similar to the CPPA proposed in Bill C-27, it incorporates several material updates.

PPCDA-specific changes from the CPPA/Bill C-27

- oversight and enforcement transferred to the new Digital Safety and Data Protection Commission of Canada (no standalone OPC or adjudicative tribunal for private sector privacy)
- no accompanying standalone legislation regulating artificial intelligence
- no standalone adjudicative tribunal to enforce the private sector privacy regime
- still no comprehensive privacy protection for personal information held by federal political parties
- personal information expressly includes inferred information about an identifiable individual (s. 2(1))
- enhanced focus on children: new statutory definition of "child" (under 18), children's personal information included within definition of "sensitive" personal information, and requirement for the Commission, Commissioner and Division to consider "best interests of children" (ss. 2(1), 77(d), 86(d), 90(d))
- legitimate interests exception extends to disclosure as well as collection and use (s. 18(3))
- new requirement to conduct a privacy impact assessment and implement mitigating measures prior to transferring or disclosing personal information outside Canada (s. 57)
- new opportunity for individuals to make written representations contesting an automated decision system output (s. 63(6))
- failing to comply with the reasonable and appropriate purposes requirement for the collection, use and disclosure of personal information is now an enumerated contravention attracting AMPs (ss. 12(1), (3), (4))
- new AMP factors: organization's ability to pay and financial benefit obtained from contravention
- no preamble (unlike the lengthy preamble in the CPPA)
- removal of the CPPA's proposed disclosure exceptions for "statistics, study or research purposes" and "socially beneficial purposes"

2

Regulatory model and enforcement

2.1 Proposed oversight and enforcement structure

Highlights

- **Key change from PIPEDA**: Oversight and enforcement shifts from the OPC to the newly created Digital Safety and Data Protection Commission of Canada, a multi-member body appointed by the Governor in Council that is not an independent agent of Parliament.
- **Key change from the CPPA**: Rather than retaining the OPC alongside a separate Tribunal, the PPCDA consolidates oversight, penalty, and initial appeal functions within the Commission. The new oversight framework is less directly tied to traditional Parliamentary oversight mechanisms, as the members of the Commission are appointed by the Governor in Council and the Commission reports through the responsible minister.

Digital Safety and Data Protection Commission of Canada (Commission)

- replaces the Office of the Privacy Commissioner of Canada for private sector privacy law regime
- overall oversight and enforcement of the PPCDA regime
- also mandated to promote online safety and reduce harms from harmful content by administering and enforcing the *Digital Safety Act* (Bill C-34) governing regulated social media, chatbot and other online services

Privacy and Consumer Data Commissioner (Commissioner)

Member of Commission · Investigative arm

- unlike under PIPEDA, the Commissioner is not an independent agent of Parliament
- investigation of complaints and self-initiated (ss. 97–100)
- compliance agreements (in course of resolving investigations) (ss. 102–103)
- notices of contravention (ss. 105–108) — must include grounds for contravention, including the provisions of PPCDA that have been contravened, any penalty or "proposed order," and information regarding right to apply for a review
  - if uncontested, deemed contravention and penalty is levied and "proposed order" is deemed to be made by Commission
  - injunctive relief (application for review to Commission) (s. 109)
  - discretion to publish information where it is in public interest (s. 135(3))
- audit/investigation powers (ss. 118, 122)
- ensures compliance with approved certification programs (s. 85)
- above processes governed by guidance that will be developed by Commission in consultation with minister and other stakeholders (s. 78)

Privacy and Consumer Data Division (Division)

Commissioner and 1+ members of Commission

- dispute resolution to resolve complaints (s. 101)
- approves codes of practice and certification programs (ss. 93–96)
- may delegate a majority of Commission responsibilities, including developing guidance, conducting research and consultation with international stakeholders relating to compliance with Act
  - minister may request guidance materials, tools and that research be conducted (s. 76)

Adjudicative function of Commission

Excludes Commissioner and any member with reasonable apprehension of bias (ss. 111, 124)

- hears applications for review of notices of contravention and interim orders issued by Commissioner (ss. 109, 123)
- reviews, confirms and varies penalties (s. 110)
- reviews, confirms or varies proposed orders included in notices of contravention issued by Commissioner, and makes orders (s. 110)
- issuance of interim orders (s. 121)
- must conduct in accordance with rules published by Commission (s. 78)

Commissioner cannot adjudicate (s. 111)

▼

Federal Court

- unlike PIPEDA, organizations can appeal decisions by Commission (ss. 126–128)

Bill C-36 transfers responsibility for federal private sector privacy law from the OPC to a newly created Digital Safety and Data Protection Commission of Canada (the Commission), which will be responsible for administering the PPCDA. The Commission will also have responsibility for the recently proposed *Digital Safety Act* (Bill C-34), which sets out a framework to govern online safety and reduce harms resulting from online content and establishes transparency and accountability requirements for operators of regulated services, such as social media sites, chatbots and other online services.

Key features of the Digital Safety and Data Protection Commission of Canada

- The Commission consists of three to five members appointed by the Governor in Council.
- One of the Commission members will be appointed as the designated Privacy and Consumer Data Commissioner (the Commissioner) to lead the oversight and enforcement of the PPCDA and to address complaints and undertake investigations (s. 85(1)).
- Decisions of the Commissioner, which will be contained in "notices of contravention," will be subject to review by the Commission on application of the organization or complainant.
- The Commissioner will form part of the dedicated Privacy and Consumer Data Division (the Division), along with at least one other member of the Commission (s. 89), which will manage dispute resolution mechanisms to resolve complaints (s. 101) and approve codes of practice and certification programs (ss. 93–96), as well as any other responsibility delegated by the Commission.
- The Commission has broad powers, duties and functions that may be delegated to the Division and Commissioner, including developing guidance materials for organizations, conducting public information programs, conducting research into the protection of personal information (including where requested by the minister), and consulting with international stakeholders on the promotion and administration of privacy and data protection issues (ss. 76–82).
- The Commission will also work with organizations upon request to review and provide guidance on the organization's privacy management programs.
- Unlike the OPC, the Commission and the Commissioner are not independent agents of Parliament.

2.2 Investigation and enforcement process

Highlights

- **Key change from PIPEDA**: Unlike the existing regime under PIPEDA, where the Privacy Commissioner's role is largely ombudsperson-style focused on investigation and non-binding recommendations to promote compliance, the new Commissioner gains broad powers to, in the course of investigations, enter into compliance agreements, issue notices of contravention, issue penalties and propose binding orders.
- **Key change from the CPPA**: The formal "inquiry" process is replaced with a streamlined model in which an uncontested notice of contravention results in a deemed contravention, with the penalty becoming due and the proposed order being made by the Commission without further review. The organization or complainant may apply to the Commission for review of any aspect of the notice, and the Commissioner cannot hear these reviews. Commission decisions may be appealed to the Federal Court. Investigations may also be resolved through dispute resolution mechanisms conducted by the Division.

Key features of the Privacy and Consumer Data Commissioner

The Commissioner operates as the investigative arm and may investigate an organization's compliance with the PPCDA, either in response to a complaint, or where they are satisfied that there are reasonable grounds to investigate a matter under the Act (ss. 97–100). The Commissioner is also responsible for reviewing an organization's compliance with approved certification programs and may conduct audits into an organization's compliance (ss. 85, 118).

Investigations can also be resolved through a dispute resolution process conducted by the Division, which will be outlined further in regulations and guidance (s. 101).

The Commissioner is granted broad investigative powers, including to order the production of documents and examine premises (s. 122).

If, in the course of an investigation, the Commissioner believes on reasonable grounds an organization has contravened a requirement of the PPCDA, the Commissioner may

- enter into a compliance agreement with the organization aimed at ensuring compliance with the Act (ss. 102–103)
- issue a notice of contravention setting out
  - the facts of the alleged contravention and the Commissioner's reasons for believing there is a contravention, as well as the provisions of the PPCDA that have been contravened
  - the penalty that an organization is liable to pay and the time and manner in which the penalty must be paid
  - the "proposed order," if any, that the Commissioner considers reasonably necessary to ensure compliance with the PPCDA and the reasons for it
  - the organization's rights regarding a review (s. 107)
- in exigent circumstances, issue interim orders (s. 122)

Where the notice of contravention is uncontested, the contravention is deemed to have occurred, and the order is made by the Commission and the penalty becomes due (ss. 108–109).

Review of orders/penalties

The organization and complainant may apply for a review of any aspect of the notice of contravention (including penalties and orders) or interim orders by the Commissioner (s. 109). The Commission will hear applications and review, confirm or vary penalties and proposed orders issued by the Commissioner, then make its decision (s. 121). The Commissioner cannot hear these reviews (ss. 111, 124).

The investigation and enforcement processes are governed by guidance that will be developed by the Commission in consultation with the designated minister and other stakeholders (s. 78).

Decisions of the Commission may be appealed by the complainant or affected organization to the Federal Court (ss. 126–128). Interim orders may be appealed only with leave (s. 127(1)).

2.3 Administrative monetary penalties (AMPs)

Highlights

- **Key change from PIPEDA**: The PPCDA introduces AMPs, which PIPEDA does not have.
- **Key change from the CPPA**: The penalty framework is substantively similar to the CPPA, but flows through the Commission rather than an independent Tribunal. New factors to be considered when issuing a penalty include the organization's ability to pay and financial benefit obtained from the contravention; affected organizations (not only complainants) may appeal to the Federal Court.

The PPCDA introduces AMPs up to the higher of $10 million or 3% of the organization's gross global revenues (s. 114). Penalties may only be imposed by the Commissioner for enumerated contraventions, as set out below (s. 113(1)).

Contravention	PPCDA provision
Failing to implement/maintain a privacy management program	s. 9(1)
Failing to ensure equivalent protection for service provider transfers	s. 11(1)
Collecting/using/disclosing personal information for purposes that are not "appropriate"	s. 12(1)
Failing to determine/record purposes before collection or new use/disclosure of personal information	ss. 12(3)–12(4)
Collecting personal information beyond what is necessary	s. 13
Using/disclosing personal information for secondary purpose without consent or exception	s. 14(1)
Failing to obtain valid consent	s. 15(1)
Contravening the "refusal to deal" provision	s. 15(7)

Contravention	PPCDA provision
Obtaining consent through deception	s. 16
Failing to inform of the consequences of withdrawing consent or failing to cease processing in respect of the withdrawal of consent	s. 17(2)
Contravening retention and disposal requirements	ss. 52, 54(1), 54(5)
Failing to safeguard personal information	s. 56(1)
Failing to report/notify breaches of security safeguards	ss. 58(1), 58(3)
Service provider failing to notify accountable entity of a breach	s. 61
Failing to make policies/practices information available	s. 62(1)

Factors in determining penalty amount

In imposing an AMP, the Commissioner/Commission must consider

- the nature and scope of the contravention
- evidence of exercise of due diligence to avoid the contravention
- whether the organization made reasonable efforts to mitigate or reverse the effects of the contravention
- history of compliance
- the organization's ability to pay the penalty and the likely effect that paying it would have on the organization's ability to carry on its business
- any financial benefit that the organization obtained from the contravention
- any other prescribed or relevant factor

The Commissioner determines penalties after investigation (ss. 105–109, 113). However, the complainant or the organization can apply for a review of these by the Commission, who may elect to vary the penalty (ss. 109–110).

An AMP cannot be imposed if the organization was in compliance with an approved certification program at the time of the contravention (s. 113(3)(a)). However, the private right of action remains available (s. 132).

2.4 Offences and criminal fines

Highlights

- **Key change from PIPEDA**: The PPCDA introduces significant criminal penalties for knowing contraventions. PIPEDA has no comparable offence provisions.
- **Key change from the CPPA**: The proposed fines remain substantively identical to those under the CPPA.

Certain knowing contraventions may be prosecuted as offences.

Offence type	Maximum fine
Summary offence	Higher of $20 million or 4% of gross global revenues (s. 145(b))
Indictable offence	Higher of $25 million or 5% of gross global revenues (s. 145(a))

Examples of conduct that may constitute an offence include

- failing to report a breach of security safeguards or notify affected individuals (s. 58)
- failing to provide the Commission with access to breach records (s. 60(1))
- failing to retain information subject to an access request (s. 69)
- unauthorized re-identification of de-identified information (s. 75)
- retaliation against a whistleblower (s. 144(1))
- contravening an order made by the Commission to ensure compliance with the PPCDA (s. 110(1))
- obstructing an investigation or audit (ss. 109, 123(4))

2.5 Order-making powers and private right of action

Highlights

- **Key change from PIPEDA**: The new Commission receives binding order-making powers to require compliance, publicize corrective measures, and make information preservation orders. The PPCDA also introduces a statutory private right of action for affected individuals following a final finding of contravention, a compliance agreement, or a conviction.
- **Key change from the CPPA**: Under the CPPA, the private right of action required either a final finding by the Commission or Tribunal that an organization had contravened the act. Under the PPCDA, claims proceed following a final Commission finding or Federal Court decision. In both frameworks, these actions may be brought in either the Federal Court or provincial superior courts.

Order making powers

In the course of an investigation, the Commission may impose binding orders on organizations to comply, and to publicize any corrective measures to ensure compliance with the Act (s. 110). In addition, during a review under ss. 109 or 123, the Commission may make any *interim order* considered appropriate and may make *information preservation orders* (ss. 121(1), 121(2)(d)).

Orders and penalties issued by the Commission may be appealed to the Federal Court, and interim orders may be appealed with leave (ss. 126, 127 (1)).

Private right of action

After a final finding of contravention, the entering of a compliance agreement or a conviction, affected individuals may sue for damages for loss or injury suffered as a result (s. 132(1)–(2)). Claims may be brought in either Federal Court or the superior courts of the provinces (s. 132(5)). A two-year limitation period runs from the final finding or conviction after all appeal rights have been exhausted (s. 132(4)).

3

Legislative intent and purpose, application and definitions

3.1 Legislative intent and purpose

Highlights

- **Key change from PIPEDA**: The PPCDA expressly articulates that privacy is a fundamental right, which was not recognized in PIPEDA or the CPPA.
- **Key change from the CPPA**: In addition to the above, the PPCDA does not include a lengthy preamble like the CPPA, and introduces a new overarching obligation for the Commission, Commissioner and the Division to exercise their powers in a proportionate and contextual manner.

Although the PPCDA does not include a preamble, the Act's operative provisions and purpose clause can be used to interpret legislative intent. The PPCDA provides that:

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

Notably, the express recognition of privacy as a "fundamental right" in the legislation, which was strongly advocated for by the OPC, is a key change from the CPPA and recognizes the significance of the rights being protected by the PPCDA and balanced against the needs of organizations.

In addition, the PPCDA provides that the Commission, the Commissioner and the Division must take into account all relevant factors when exercising their powers or performing their duties or functions, including

- the size and revenue of organizations
- the volume of personal information under the control of organizations and the sensitivity of that information
- the best interests of children
- the importance of respecting Canada's international trade obligations
- the importance of supporting economic growth, competition and innovation in the Canadian marketplace
- any other matter of general public interest (ss. 77, 86, 90)

This provision builds proportionality and a contextual analysis into the regulatory framework in a more express manner than under PIPEDA.

3.2 Application

Highlights

- **Key change from PIPEDA**: The application of the PPCDA has not materially changed from PIPEDA. The PPCDA maintains the definition of "commercial activity" as set out in PIPEDA and the CPPA.
- **Key change from the CPPA**: None or not material.

Like PIPEDA, the PPCDA applies to the collection, use and disclosure of personal information in the course of commercial activities, and to personal information of employees and job applicants of federal works, undertakings and businesses.

The PPCDA includes PIPEDA's definition of "commercial activity," meaning "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists" (s. 2(1)).

The PPCDA does not apply to certain information, including the following

- personal information that the organization collects, uses and discloses outside the scope of the organization's commercial activities (s. 6(1))
- anonymized information (s. 6(5))
- personal information collected, used or disclosed for personal, journalistic, artistic or literary purposes (ss. 6(4)(b)–(c))
- personal information collected, used or disclosed solely for the purpose of communicating with an individual in relation to their employment, business or profession (s. 6(4)(d))
- employee personal information in the context of provincially regulated employment relationships

3.3 Key definitions

Highlights

- **Key change from PIPEDA**:
  - The PPCDA clarifies that personal information includes inferred information about an identifiable individual.
  - The PPCDA introduces a non-exhaustive definition of sensitive personal information that requires a contextual analysis and that specifically identifies certain personal information that may be sensitive, including children's information and health information. PIPEDA, on the other hand, does not include a specific definition but similarly provides that personal information may be considered sensitive depending on the context.
  - The PPCDA introduces specific definitions to account for different states of data, including de-identified personal information and anonymous information, which are not expressly defined in PIPEDA.
- **Key change from the CPPA**:
  - The PPCDA clarifies that personal information includes inferred information about an identifiable individual.
  - While the CPPA recognized that the personal information of a minor and certain medical information would be considered sensitive, the CPPA was otherwise silent on the scope of sensitive personal information.
  - The PPCDA includes a revised definition of "anonymize" to that which was originally introduced by the CPPA.

The PPCDA includes key terms that define different types of personal information and other data.

Personal information

Under the PPCDA, the definition of personal information has been clarified to include "information that is inferred about [the identifiable individual]" (s. 2(1)). The express mention of inferred information in the definition is new.

Sensitive personal information

The PPCDA introduces a definition of "sensitive," which describes personal information in respect of which, taking into account the circumstances, an individual has a heightened expectation of privacy, including, as the case may be:

- a child's personal information
- personal information revealing an individual's racial or ethnic origin, political opinions or religious or philosophical beliefs
- an individual's trade union membership
- genetic information or health information
- biometric information that is capable of uniquely identifying an individual or
- information concerning an individual's sexual orientation (s. 2(1))

De-identified personal information

The PPCDA uses essentially the same definition of de-identified personal information as set out in the CPPA, meaning personal information that has been modified "so that an individual cannot be directly identified from it, although a risk of the individual being identified remains" (s. 2(1)).

The PPCDA provides that all de-identified personal information remains personal information under the PPCDA (s. 2(2)). However, certain obligations under the PPCDA do not apply to de-identified personal information. Specifically, organizations are not required to fulfil the following rights requests in respect of de-identified personal information: disposal; information and access; amendment; and data mobility (ss. 51(3), 63(2), 71(2), 72(2)). Further, the obligation to maintain accuracy does not apply to de-identified personal information (s. 55(2)).

When de-identifying personal information, organizations must consider re-identification risk when applying technical and administrative measures, and ensure those measures are proportionate to the purpose for which the information is de-identified and its sensitivity (s. 74).

Organizations are prohibited from using de-identified personal information — alone or in combination with other information — to identify an individual, except in specified circumstances, including testing the effectiveness of security safeguards, testing the fairness and accuracy of models developed using de-identified personal information, testing de-identification effectiveness and, as an expansion to the CPPA, in circumstances where the personal information was de-identified solely for the purpose of protecting it, where the organization has valid consent or where the organization is otherwise able to rely on a defined exception to consent (s. 75). Knowingly contravening section 75 is an offence that is subject to significant fines.

Anonymized information

Under the PPCDA, "anonymize" means "to irreversibly and permanently modify personal information to ensure that 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" (s. 2(1)). This change to the definition of "anonymize" brings the term into alignment with the standard for anonymization in legislative schemes across Canadian and certain global jurisdictions. Like the CPPA, the PPCDA confirms that anonymized information falls outside the application of the Act (s. 6(5)).

4

Key obligations by theme

4.1 Reasonable and appropriate purposes

Highlights

- **Key change from PIPEDA**: The PPCDA retains PIPEDA's reasonable person standard for appropriate purposes, but would now introduce a non-exhaustive list of factors for assessing appropriateness and make a breach of the standard subject to monetary penalties.
- **Key change from the CPPA**: The factors are now illustrative rather than exhaustive, and the appropriate purposes standard (which the CPPA left outside the penalty regime) is now subject to a monetary penalty.

Section 12(1) of the PPCDA carries forward PIPEDA's reasonable person standard: 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." Section 12(2) sets out a non-exhaustive list of factors to be taken into account, if applicable, in making a determination on appropriateness:

- the sensitivity of the 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
- 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

This approach largely codifies the four-part reasonableness analysis developed by courts under PIPEDA and that formed the basis for the OPC's Guidance on inappropriate data practices.

A contravention of section 12(1) is now subject to a penalty of up to the higher of $10 million or 3% of gross global revenue (ss. 113(1)(c), 114).

4.2 Purpose identification and data minimization

Highlights

- **Key change from PIPEDA**: The PPCDA carries forward PIPEDA's duties to identify and document collection purposes and limit collection to what is necessary, but recasts them as binding obligations backed by monetary penalties.
- **Key change from the CPPA**: None or not material.

Sections 12(3) and (4) require an organization to determine, at or before the time of collection, the purposes for which personal information *is or is to* be collected, used and disclosed, and to record these purposes (s. 12(3)). Any new purpose must be recorded before using or disclosing personal information for the new purpose (s. 12(4)).

Section 13 limits collection to the personal information that is "necessary" for the purposes recorded under s. 12(3).

These obligations largely restate existing PIPEDA requirements to identify, document and limit collection, but replace them in binding provisions of the Act rather than in Schedule 1 under PIPEDA. Section 13 does not carry forward PIPEDA's requirement that information be collected by "fair and lawful means."

Collection of personal information beyond what is necessary can attract penalties of up to the higher of $10 million or 3% of gross global revenue (ss. 113(1)(c)–(d), 114).

4.3 Accountability provisions

Highlights

- **Key change from PIPEDA**: The PPCDA introduces a statutory obligation to implement a privacy management program, and to provide access to its privacy policies, practices, and procedures to the Commission upon request.
- **Key change from the CPPA**: None or not material.

The PPCDA clarifies the concept of an "accountable organization" and sets out several provisions relating to demonstrable accountability. Similar to PIPEDA, organizations are "accountable" for personal information under their control (s. 7(1)). The PPCDA clarifies that personal information is under the control of an organization that "decides to collect it and that determines the purposes for its collection, use or disclosure, regardless of whether the information is collected, used or disclosed by the organization itself or by a service provider on behalf of the organization" (s. 7(2)).

Organizations are required to designate one or more individuals as responsible for compliance with the Act (s. 8(1)). They must also implement and maintain a privacy management program that includes policies, practices and procedures to fulfill their obligations under the Act and that takes into account the volume and sensitivity of personal information under their control (ss. 9(1)–(2)).

Upon request (i.e., without needing reasonable grounds), the Commission may require organizations to provide access to their privacy management program materials (s. 10(1)). After review, the Commission may provide guidance or recommend corrective measures (s. 10(2)). Organizations may also voluntarily request guidance regarding their program (s. 76(c)(v)).

Importantly, the Commissioner cannot use information obtained through the program review mechanism (s. 10 or s. 76(c)(v)) to initiate a complaint or carry out an audit, unless the Commissioner considers that the organization has willfully disregarded the corrective measures recommended in relation to its program (ss. 10(1), 76(c)(v), 87).

Failure to implement or maintain a privacy management program is an enumerated contravention attracting penalties of up to the higher of $10 million or 3% of gross global revenue (s. 113(1)(a)).

4.4 Service providers

Highlights

- **Key change from PIPEDA**: The PPCDA introduces a definition of "service provider" and clarifies the obligations applicable to service providers. PPCDA also codifies existing OPC guidance that a transfer to a service provider is not a disclosure of personal information that requires consent. Organizations must, however, ensure contractual or other means are in place to ensure an equivalent level of protection.
- **Key change from the CPPA**: None or not material.

The PPCDA introduces a new definition of "service provider," which means an organization, including a parent corporation, subsidiary, affiliate, contractor or subcontractor, that provides services for or on behalf of another organization to assist the organization in fulfilling its purposes (s. 2(1)).

Service providers are only directly subject to the PPCDA's safeguarding requirements, and obligation to notify the accountable organization of a breach of security safeguards as soon as feasible (ss. 56, 61). Service providers are not subject to other obligations — including those relating to accountability, consent, retention, accuracy, rights of access, transparency, data mobility and other requirements — in respect of personal information transferred to it by an accountable organization (s. 11(2)). However, a service provider that collects, uses or discloses personal information for any purpose other than the purposes for which the information was transferred to it becomes an accountable organization subject to all of the obligations under the PPCDA (s. 11(2)).

Accountable organizations that transfer personal information to service providers do not need to obtain the consent of the concerned individuals for the transfer (s. 19). However, they must ensure, by contract or otherwise, that the service provider provides a level of protection "equivalent" to that which the organization is required to provide under the Act (s. 11(1)). This is a higher standard than under PIPEDA, which requires a "comparable" level of protection.

Where an organization disposes of personal information at an individual's request, it must inform any service provider to which it has transferred the information and ensure that the service provider disposes of the information (s. 54(5)).

Failure to ensure equivalent protection is an enumerated contravention attracting penalties of up to the higher of $10 million or 3% of gross global revenue (s. 113(1)(b)).

4.5 Transfers and disclosures outside Canada

Highlights

- **Key change from PIPEDA**: New requirements to conduct a privacy impact assessment and implement risk mitigation measures before transferring personal information outside Canada.
- **Key change from the CPPA**: The PPCDA's cross-border transfer privacy impact assessment requirement was not included in the CPPA.

Before transferring or disclosing personal information outside of Canada, organizations must

- carry out a privacy impact assessment in accordance with prescribed requirements (s. 57(1)(a))
- implement measures to mitigate risks identified in the assessment (e.g., contractual safeguards, adherence to an approved code of practice or certification program, or other prescribed measures) (s. 57(1)(b))
- provide a copy of the assessment to the Commission upon request (s. 57(2))

The organization must also be transparent about whether or not it transfers or discloses personal information interprovincially or outside of Canada that may have foreseeable privacy implications (s. 62(2)), as detailed in the "Openness and Transparency" section below.

While the PPCDA does not prescribe model clauses to be used for international data transfers, it does contemplate that the Commission may work with any person to develop model contracts or other documents relating to the interprovincial or international transfer of personal information (s. 81(2)(c)).

4.6 Codes of practice and certification programs

Highlights

- **Key change from PIPEDA**: While PIPEDA contemplated the concept of codes of practice by mandating the Commissioner to "encourage" organizations to develop codes of practice to comply with their statutory obligations, the PPCDA provides an enhanced statutory recognition of both codes of practice and certification programs. (ss. 92–96)
- **Key change from the CPPA**: The PPCDA codes of practice and certifications provisions are substantially similar to those under the CPPA.

The PPCDA provides statutory recognition of codes of practice and related certification programs (ss. 92–96).

The key criteria for codes and certification programs will be set out in regulations, but the substance of any code or certification program must provide "substantially the same or greater protection of personal information as some or all of the protection provided" under the PPCDA (s. 93(1)). Certification programs run by entities will need to include independent verification mechanisms and disciplinary measures for non-compliance with the code (ss. 93(1)(d), 93(2)).

Entities, including government institutions and any organization, may apply to the Division for approval of a code or certification program (ss. 92(2), 93(1)). The Division may formally grant approval if it is satisfied that the code or certification program meets the criteria set out in the regulations (ss. 92(3), 93(2)). The decision by the Division must be issued within the time frame set out in the regulations and must be made public (ss. 94 and 95).

Compliance with a code or certification program does not relieve an organization of its obligations under the PPCDA (s. 96).

The PPCDA provides the Commissioner with powers to request information from an entity operating an approved certification program, cooperate with an entity operating an approved certification program, recommend to the entity that an organization's certification be withdrawn in prescribed circumstances, and revoke the approval of a certification program, in prescribed circumstances as set out in regulations (ss. 85(2)(a)–(d)).

The Commissioner also has the power to decline to investigate a complaint where, among other grounds, the complaint raises an issue covered by an approved certification program and the organization is certified under that program (s. 98(1)).

Of note, a penalty cannot be imposed if an organization was in compliance with an approved certification program at the time of the contravention (s. 113(3)(a)). However, the private right of action is still available for the contravention (s. 132).

4.7 Children's personal information

Highlights

- **Key change from PIPEDA**: The PPCDA introduces a definition of "child" (defined as "an individual who is under 18 years of age") and includes a child's personal information within the definition of "sensitive".
- **Key change from the CPPA**: The PPCDA introduces a "best interests of children" factor that the Commission, Commissioner and Division must consider in exercising their powers.

PPCDA introduces express provisions regarding children's personal information.

Definition of a "child"

PPCDA defines a "child" as an individual who is under 18 years of age (s. 2(1)) and includes a child's personal information within the definition of "sensitive" (s. 2(1)).

The sensitivity of information impacts certain requirements under the PPCDA, including those relating to privacy management programs, "appropriate" purposes, form of consent, retention periods, security safeguards, breach reporting and notification, transparency, and de-identification technical and administrative measures (ss. 9(2), 12(2)(a), 15(5), 52(2), 56(1), 58(8)(a), 62(2)(e), 74(b)).

Rights and recourse

The PPCDA contains protections specific to children. While there is no express parental consent requirement, rights and recourse under the Act could be exercised on a child's behalf by a parent, guardian or tutor, unless the child wishes to exercise those rights personally and is capable of doing so (s. 4(a)).

Children also benefit from a stronger right of disposal: an organization cannot refuse a request to dispose of a child's personal information on the basis that disposal would have an undue adverse effect on the accuracy or integrity of information necessary to the ongoing provision of a product or service to the individual (s. 54(2)(d)).

Best interests of children

The "best interests of children" is a mandatory interpretive factor that the Commission, the Commissioner and the Division must each consider in exercising their powers or performing duties or functions under the PPCDA (ss. 77(d), 86(d), 90(d)).

While there is no penalty specifically tied to any requirement relating to children's data, not appropriately accounting for the sensitivity of this information could result in a finding that an organization had failed to comply with consent, transparency, accountability, breach reporting, or other requirements under the PPCDA, and may result in an organization being exposed to the imposition of a penalty up to the higher of $10 million or 3% of gross global revenue (s. 113(1)(g)).

4.8 Consent requirements and withdrawal

Highlights

- **Key change from PIPEDA**: The definition of a valid consent has been removed and replaced with more prescriptive requirements for notice at or before the time of collection for a consent to be valid.
- **Key change from the CPPA**: No material change.

Under the PPCDA, organizations may only collect, use or disclose personal information with consent, unless a statutory exception applies (s. 15(1)). This approach entrenches consent as the primary legal authority under the Act for processing personal information, as it was under PIPEDA.

Form of consent

The PPCDA establishes that the default form of consent required to collect, use and disclose personal information must be "expressly obtained" (i.e., opt-in consent) (ss. 15(1), 15(5)). Implied consent operates as an exception to this general requirement and may only be relied upon where "appropriate," taking into account an individual's reasonable expectations and the sensitivity of the personal information (s. 15(4)). This approach to consent is broadly consistent with how the OPC has interpreted and enforced PIPEDA's consent requirements.

The PPCDA further provides that reliance on implied consent is "not appropriate" if the personal information is collected or used under a consent exception for prescribed "business activities" or the personal information is collected, used or disclosed under a consent exception for "legitimate interests" (s. 15(6)). See Exceptions to consent.

Requirements for valid consent

The PPCDA introduces specific requirements regarding both the substance and accessibility of the information organizations must provide to individuals when seeking consent for the collection, use or disclosure of their personal information. Under the PPCDA, organizations must, at or before the time consent is obtained, and in "plain language," provide the following information to individuals:

- the purposes for the collection, use or disclosure as determined and recorded under sections 12(3) or (4) of the PPCDA
- the manner in which the personal information is to be collected, used or disclosed
- any reasonably foreseeable consequences
- the specific type of personal information to be collected, used or disclosed

- the names of any third parties or types of third parties to which the organization may disclose the information (ss. 15(3)–(4))

These requirements reflect guidance previously published by the OPC in its *Guidelines for obtaining meaningful consent* as well as the meaning of a "valid" consent under PIPEDA which requires that an individual understand the "nature, purpose and consequences" of the collection, use or disclosure of their personal information.

Consent obtained through deception

The PPCDA introduces an expanded prohibition against organizations obtaining — or attempting to obtain — an individual's consent by providing false or misleading information or using deceptive or misleading practices (s. 16). Any consent obtained through such means will be considered invalid and cannot be relied upon by an organization as a lawful authority for its collection, use or disclosure of personal information.

An organization that violates this prohibition may be exposed to the imposition of a penalty up to the higher of $10 million or 3% of gross global revenue (s. 113(1)(g)).

Withdrawal of consent

Similar to PIPEDA, the PPCDA recognizes that individuals may, on giving reasonable notice to the organization, withdraw their consent to the collection, use or disclosure of their personal information, subject to the PPCDA, federal or provincial law, and the reasonable terms of a contract (s. 17(1)). Organizations must inform individuals of the consequences of their withdrawal, and as soon as is feasible, cease the collection, use or disclosure of the personal information to which the withdrawal relates (s. 17(2)).

4.9 Exceptions to consent (including business activities and legitimate interest)

Highlights

- **Key change from PIPEDA**: The PPCDA introduces new exceptions to consent for the collection and use of personal information for certain prescribed business activities and the collection, use and disclosure of personal information where the organization has a legitimate interest that outweighs reasonably foreseeable adverse effects.
- **Key change from the CPPA**: The PPCDA extends the legitimate interests exception to disclosure in addition to collection and use, which were already contemplated in the exception under the CPPA. In addition, under the CPPA, the relevant threshold referred to "any potential adverse effect," whereas the PPCDA adopts the more calibrated formulation "any reasonably foreseeable adverse effect that could result from" the collection, use or disclosure, which may afford organizations somewhat greater flexibility in relying on the exception.

Business activities

The PPCDA introduces a new exception to consent for the collection and use of personal information for standard business activities (s. 18(1)). Organizations may rely upon this exception for their use — but not disclosure — of personal information where such use falls within the scope of business activities contemplated by section 18(2). However, reliance on this exception is subject to two cumulative conditions:

- the collection must be for a purpose that a reasonable person would expect (s. 18(1)(a))
- the personal information at issue must not be collected or used "for the purpose of influencing the individual's behaviour or decisions" (s. 18(1)(b))

The prescribed business activities are drafted in technology-neutral terms and are non-exhaustive, as additional activities may be added by regulation. At present, the activities include

- activities necessary to provide a product or service requested by the individual
- activities necessary to protect the security of the organization's information; systems or networks
- activities necessary to ensure the safety of a product or service provided by the organization. Once enacted, this exception will provide organizations with a statutory basis for operational processing activities that were previously addressed through reliance on implied consent under PIPEDA.

Legitimate interests

The PPCDA introduces a new exception permitting organizations to collect, use or disclose personal information without consent where the processing is for the purpose of an activity in which the organization has a legitimate interest that outweighs any reasonably foreseeable adverse effect on the individual (s. 18(3)). Reliance on this exception is subject to two cumulative conditions:

- a reasonable person would expect the collection, use or disclosure for such an activity
- the personal information is not collected, used or disclosed for the purpose of influencing the individual's behaviour or decisions (ss. 18(3)(a)–(b))

Once an organization has determined that its intended collection, use or disclosure of personal information will satisfy the conditions mentioned above, the PPCDA requires that the organization take additional steps including

- identify and describe its legitimate interest in the proposed activity
- carry out, in accordance with the prescribed requirements, a privacy impact assessment in which the organization must identify any reasonably foreseeable adverse effect on the individual that is likely to result from the collection, use or disclosure
- identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them (s. 18(4))

The organization must maintain a record of the description of its legitimate interest, and a copy of this record must be provided to the Commissioner upon request (s. 18(5)).

Service provider transfers

The PPCDA introduces an express statutory exception to the consent requirement for transfers of personal information to service providers (s. 19). This provision largely codifies the OPC's longstanding position under PIPEDA that a transfer of personal information to a service provider, where the information is used only for the purposes for which it was originally collected, is generally considered a use by the organization rather than a disclosure requiring separate consent.

Organizations must comply with accountability obligations when transferring personal information to a service provider. See Service providers.

De-identification and anonymization

The PPCDA creates an express exception to consent that permits organizations to use personal information to de-identify or anonymize the information (s. 20).

Internal research, analysis and development

The PPCDA provides an exception to the consent requirement for the use of personal information for an organization's internal research, analysis and development purposes, provided that the information is de-identified (in accordance with the standard under the PPCDA) before being used for such purposes (s. 21). The scope of "internal research, analysis and development purposes" is broad and therefore could be interpreted to include activities such as analytics, artificial intelligence, machine learning and other data-driven development activities.

Business transactions

The PPCDA sets out an exception to the consent requirement for the use and disclosure of personal information in connection with prospective or completed business transactions (s. 22). Similar to PIPEDA, this provision permits parties to a transaction to share personal information where specified conditions are met, including requirements relating to safeguarding the information and providing notice to affected individuals following completion of the transaction.

However, the PPCDA significantly narrows this exception by requiring that personal information be de-identified before it is used or disclosed in connection with a prospective transaction and remain de-identified until completion of the transaction.

This de-identification requirement does not apply where

- de-identification would undermine the objectives of carrying out the transaction
- the organization has taken into account the risk of harm to the individual that could result from the use or disclosure of the information (s. 22(2))

Fraud detection

The PPCDA introduces an express exception to the consent requirement for collection and use of personal information for the purposes of detecting, suppressing or preventing fraud (s. 27(2)). This provision addresses a technical gap in PIPEDA's fraud-related exception, which expressly permitted disclosure of personal information to another organization for these purposes but did not contain a corresponding exception for the collection or use of personal information.

Anti-money laundering and terrorist financing disclosure

Similar to PIPEDA, the PPCDA contains a consent exception permitting the disclosure (and corresponding collection and use) of personal information without consent where the disclosure is made to another organization in accordance with section 11.01(1) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (s. 41).

A failure to obtain valid consent, or to use or disclose personal information for a secondary purpose without consent (or the application of an exception) (s. 14(1); s. 15(1)) could expose an organization to the imposition of a penalty up to the higher of $10 million or 3% of gross global revenue (s. 113(1)(f)).

4.10 Transparency and openness

Highlights

- **Key change from PIPEDA**: The PPCDA imposes a greater standard for information about an organization's privacy policies and practices to be provided to individuals in "plain language", rather than in a form that is "generally understandable". The PPCDA expands the information that must be made available to individuals.
- **Key change from the CPPA**: The PPCDA transparency and openness provisions are substantially similar to those under the CPPA.

The PPCDA requires organizations to make information explaining their policies and practices "readily available, in plain language" (s. 62(1)). PIPEDA imposes a lesser standard that requires organizations to be open about policies and to make information readily available in a form that is "generally understandable" (Schedule 1, Principle 4.8).

The PPCDA supplements PIPEDA's transparency requirements by setting out the following new mandatory content (s. 62(2))

- how the organization applies consent exceptions, including a description of any processing based on legitimate interest (s. 62(2)(b))
- a general account of any automated decision systems used to make predictions, recommendations or decisions about an individual that could have a legal or similarly significant effect on individuals (s. 62(2)(c))
- whether the organization transfers or discloses personal information interprovincially or outside Canada with reasonably foreseeable privacy implications (s. 62(2)(d))
- retention periods applicable to sensitive personal information (s. 62(2)(e))
- how individuals may request disposal of their information (s. 62(2)(f))

In addition, the transparency requirement under the PPCDA requires organizations to provide notice about the organization's policies and practices put in place "to fulfill its obligations under this Act." The latter phrase is distinct from PIPEDA, which provides that organizations must provide notice about its policies and practices "with respect to the management of personal information."

Failure to comply with the openness and transparency obligations in section 62(1) of the PPCDA is an enumerated contravention attracting penalties of up to the higher of $10 million or 3% of gross global revenue (ss. 113(n), 114).

4.11 Automated decision systems

Highlights

- **Key change from PIPEDA**: The PPCDA introduces requirements related to automated decision systems.
- **Key change from the CPPA**: The PPCDA now includes a right for individuals to submit representations to an employee of the organization able to review the decision. The PPCDA requires that organizations consider the "legal or similarly significant effect" on individuals rather than "significant impact" when providing a general account of the organization's use of any automated decision system to make predictions, recommendations or decisions about individuals.

Like other modern privacy law frameworks, including the Québec *Act respecting the protection of personal information in the private sector* (the Québec Privacy Act), the PPCDA introduces requirements regarding the use of "automated decision systems," defined as "any technology that assists or replaces the judgement of human decision makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning and a neural network or other technique" (s. 2(1)). The use of the word "assist" indicates that these requirements are not limited to fully automated decisions — for example, an algorithm used to flag applications for human review could potentially fall within scope.

Where automated decision systems are used to make predictions, recommendations or decisions about individuals that could have a legal or similarly significant effect, the following requirements are triggered:

- **Openness**: Organizations must make readily available a general account of their use of any such system as part of their transparency and openness obligations (s. 62(2)(c)).
- **Access/explanation**: Upon request, organizations must provide a plain language explanation of any prediction, recommendation or decision, which must indicate the type of personal information used, the source of the information, and the reasons or principal factors that led to the prediction, recommendation or decision (ss. 63(4)–(5), 66(1)).
- **Written representations**: Provide the individual with an opportunity to make written representations to an employee who can review the prediction, recommendation or decision (s. 63(6)). This requirement was not found in the CPPA, though it mirrors a requirement of the Québec Privacy Act.

Unlike certain international privacy frameworks, for example the E.U.'s *General Data Protection Regulation* (GDPR), the PPCDA does not provide an express right to object to automated decisions.

Failure to comply with openness and transparency obligations regarding the use of automated decision systems could cause an organization to be exposed to the imposition of a penalty up to the higher of $10 million or 3% of gross global revenue (s. 113(1)(n)).

4.12 Breaches of security safeguards

Highlights

- **Key change from PIPEDA**: The PPCDA introduces a statutory obligation for service providers to notify the organization that controls the information of a breach of security safeguards.
- **Key change from the CPPA**: None or not material.

The PPCDA contains a security breach notification framework that remains substantially similar to the current PIPEDA regime.

Organizations must report to the Commission and notify affected individuals of any breach of security safeguards involving personal information under their control where it is reasonable in the circumstances to believe the breach creates a "real risk of significant harm" to an individual (s. 58). Both the report and the notification are required as soon as feasible after the organization determines the breach has occurred. Whether the threshold is met turns on the sensitivity of the information, the probability of misuse and any other prescribed factor (s. 58(8)).

Where another organization or government institution may be able to reduce the risk of harm, the organization must also notify it (s. 59). Separately, organizations must keep a record of every breach, regardless of whether the "real risk of significant harm" threshold is met (s. 60).

PPCDA codifies the obligation on a service provider to notify the organization that controls the information as soon as feasible after determining that a breach of security safeguards has occurred, and this obligation is not qualified by the "real risk of significant harm" threshold (s. 61).

Form, content and recordkeeping requirements are left to regulation.

The Commission may impose penalties for breaching the notification requirements (s. 58) or safeguarding requirements (s. 56(1)), with fines of up to the higher of $10 million or 3% of gross global revenues (s. 113(1)). Knowing contraventions of the breach notification (s. 58) or recording requirements (s. 60(1)) may be prosecuted as offences, carrying fines of up to the higher of $25 million or 5% of gross global revenues (s. 145).

4.13 Rights of information, access and amendment

Highlights

- **Key change from PIPEDA**: The PPCDA gives individuals substantially the same rights of access to, and amendment of, their personal information. De-identified information is excluded from the scope of the access and amendments rights right.
- **Key change from the CPPA**: Unlike the PPCDA, the CPPA did not exclude de-identification from the scope of the access right.

Like PIPEDA, the PPCDA gives individuals a right to access the personal information an organization holds about them and to have inaccurate information corrected.

On request, an organization must inform the individual whether it holds personal information about them, how it uses and discloses the information, and give the individual access to that information (s. 63(1)). If the organization has disclosed the information, the organization must identify the third parties or types of third parties to which the disclosure was made (s. 63(3)).

An organization is not required to act on an access request in respect of de-identified personal information (s. 63(2)).

Form of request, assistance and plain language

Like PIPEDA, the PPCDA provides that a request must be made in writing, and the organization must assist any individual who needs help preparing a request (s. 64). The organization must provide the requested information in plain language and give access in an alternative format to an individual with a sensory disability where a version already exists or its conversion is reasonable and necessary (s. 66(1)–(2)).

Time limits and cost

An organization must respond with due diligence and no later than 30 days after receiving the request (s. 67(1)), with the possibility to extend that time limit for a maximum of 30 days in limited circumstances, which are essentially unchanged from PIPEDA (s. 67(2)).

An organization that refuses a request must give written reasons and advise the individual of available recourse; a failure to respond within the time limit is deemed a refusal (ss. 67(3)–(4)). An organization must not charge for responding to a request unless it has informed the individual of the approximate cost and the cost is minimal (s. 68).

Refusal of access

The PPCDA substantially preserves the exceptions to access set out in PIPEDA (ss. 70(1), 70(7)).

Amendment of personal information

Where an individual has been given access to their personal information and demonstrates that it is not accurate, up to date or complete, the organization must amend the information as required (s. 71(1)). An organization is not required to amend de-identified personal information (s. 71(2)). Where appropriate, the organization must transmit the amended information to any third party with access to it (s. 71(3)). Where the organization and individual do not agree on the amendments, the organization must record the disagreement and, where appropriate, inform such third parties of it (s. 71(4)).

Penalties

The access and amendment provisions (ss. 63–71) are not enumerated contraventions attracting administrative monetary penalties under section 113(1). However, knowingly failing to retain information that is the subject of an access request (s. 69) may be prosecuted as an offence, exposing an organization to a fine of up to the higher of $25 million or 5% of gross global revenues on indictment (s. 145).

4.14 Right of disposal (deletion)

Highlights

- **Key change from PIPEDA**: The PPCDA introduces a right to request disposal of personal information.
- **Key change from the CPPA**: The PPCDA introduces a ground to refuse a disposal request where disposal would have an undue adverse effect on the organization that outweighs potential adverse effects of retention on the individual.

The PPCDA establishes a statutory right of disposal of personal information. In a technical briefing held shortly after the introduction of Bill C-36 (on June 17, 2026), Government of Canada representatives framed this right as a "new right to request deletion," including to enable Canadians to ask that an organization "take down" deepfakes based on their likeness.

A new statutory right

On an individual's written request, an organization is required to dispose of that individual's personal information where

- the information was collected, used or disclosed in contravention of the PPCDA
- the individual has withdrawn consent, in whole or in part, to its collection, use or disclosure; or
- the information is no longer necessary for the continued provision of a product or service the individual requested (s. 54(1)(a)–(c))

To "dispose" means to permanently and irreversibly delete personal information or to anonymize it (s. 2(1)). Disposal must occur "as soon as feasible" after the request, and the organization must inform any service provider to which it transferred the information "as soon as feasible" of the request and ensure that the service provider also disposes of it (ss. 54(1), 54(5)).

PIPEDA does not contain an express, standalone right to request disposal. Under PIPEDA, organizations may only retain personal information for as long as necessary to fulfil identified purposes and must thereafter destroy, erase or anonymize the information, and individuals have the right to withdraw their consent to the collection, use or disclosure of their personal information, subject to legal or contractual restrictions. In some circumstances, the right to withdraw consent effectively results in a corresponding obligation to delete the individual's personal information where the organization no longer has any purpose for retaining it.

Refusal of requests

Where a request to dispose of personal information is grounded in the individual's withdrawal of consent or information no longer being necessary (and not grounded in the collection, use or disclosure taking place in contravention of the Act), an organization may refuse disposal where

- it would also dispose of another individual's personal information that cannot be severed without imposing an undue burden on the organization
- legislative requirements or reasonable terms of a contract prevent disposal
- the information is necessary for the organization to establish a legal defense or exercise other legal remedies
- the information does not relate to a child and disposal would have an undue adverse effect on the accuracy or integrity of information necessary to the ongoing provision of a product or service to the individual
- the request is vexatious or made in bad faith; or
- disposal would have an undue adverse effect on the organization that outweighs any potential adverse effect on the individual resulting from the retention of the information (ss. 54(2)(a)–(f))

An organization is not required to dispose of de-identified personal information (s. 54(3)). This exemption has no analogue in PIPEDA, which does not address disposal of de-identified information.

Where an organization refuses a request, it must inform the individual in writing, setting out the reasons and any recourse the individual may have — that is, to challenge compliance or to file a complaint with the Commissioner (ss. 54(4)(a), 73, 97(1)).

Where an organization refuses a request on the basis that the disposal would have an undue adverse effect on the organization that outweighs any potential adverse effect on the individual resulting from the retention of the information, the organization would also be required to inform the Commission (ss. 54(2)(f), 54(4)(b)).

This balancing test and notice provision replaces a refusal ground under the CPPA that would have permitted refusal where information that did not relate to a minor was already scheduled for disposal under the organization's retention policy and the organization informed the individual of the remaining period for which the information would be retained.

Contravention of requirements relating to retention and disposal periods, compliance with disposal requests, and ensuring service provider compliance with disposal requests could expose an organization to a penalty of up to the higher of $10 million or 3% of gross global revenues (ss. 114, 52, 54(1), 54(5)).

4.15 Right of data mobility

Highlights

- **Key change from PIPEDA**: The PPCDA carries forward substantially the same provisions that were first introduced as an amendment to PIPEDA via Bill C-15 (*Budget 2025 Implementation Act, No. 1*), which received Royal Assent on March 26, 2026. The PPCDA expands on the data mobility language in Bill C-15 to include a prescribed exception for de-identified information.
- **Key change from the CPPA**: None or not material.

The PPCDA introduces a concept of a data mobility right (similar to the statutory portability rights under the Québec Privacy Act and under the GDPR). This new right requires an organization that has collected personal information from an individual to disclose such personal information to another organization "as soon as feasible" upon the individual's request.

The data mobility right is subject to a "data mobility framework" prescribed by regulations to be drafted by the Governor in Council. The disclosing and receiving organizations would both need to be subject to the data mobility framework for the disclosure to take place. These regulations will establish safeguards that must be put in place to enable the secure disclosure (and corresponding collection) of personal information, as well as prescribed technical interoperability parameters and exceptions to the disclosure requirement.

The regulations will also specify certain organizations that will be subject to a data mobility framework and may distinguish among different "classes" of "activities, government institutions or parts of government institutions, information, organizations or entities" (s. 141).

Of note, the PPCDA expressly provides that an organization is not required to disclose de-identified personal information.

Open banking is the first federal use case operationalizing the data mobility provisions under PIPEDA. The federal government passed the *Consumer-Driven Banking Act* (CDBA) in 2024. The CDBA creates a framework to both enable consumers, including small businesses, to securely share prescribed types of financial data among defined participating entities, and to foster competition in the financial sector in the interests of consumers.

About Osler, Hoskin & Harcourt LLP

Osler is a leading law firm with a singular focus — your business. From Toronto, Montréal, Calgary, Ottawa, Vancouver and New York, we advise our Canadian, U.S. and international clients on an array of domestic and cross-border legal issues. Our collaborative "one firm" approach draws on the expertise of over 600 lawyers to provide responsive, proactive and practical legal solutions driven by your business needs. For over 160 years, we've built a reputation for solving problems, removing obstacles, and providing the answers you need, when you need them.

Disclaimer

This document is intended to provide general information regarding Bill C-36 and the proposed PPCDA as introduced at first reading. It does not constitute legal advice and should not be relied upon as a substitute for obtaining legal advice specific to your organization's circumstances.

Osler, Hoskin & Harcourt LLP
Toronto Montréal Calgary Vancouver Ottawa New York | **osler.com**

OSLER