# Ten Key Considerations for Organizations on Bill C-36

Deeth Williams Wall

Richard Austin, M. Imtiaz Karamat, and Uday Bahal October 13, 2026

## Introduction

*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") was introduced in the House of Commons by the Government of Canada earlier this year. It enacts the *Protecting Privacy and Consumer Data Act* ("PPCDA"), which would repeal Part I of the *Personal Information Protection and Electronic Documents Act* and significantly update the federal privacy protection regime in Canada.

This advisory ("Advisory") identifies certain of the most significant changes to Canadian privacy law that will be implemented under the PPCDA should it be enacted in its current form.

## Overview

This advisory is divided into the following parts.

1. New Oversight and Enforcement Regime
2. Privacy Management Program Requirements
3. Updated Consent Framework
    A. New Consent Requirements
    B. Business Activities and Legitimate Interest Exceptions
4. Cross-Border Information Transfer Requirements
5. Automated Decision System Requirements
6. Enhanced Privacy Safeguards for Children
7. Anonymization and De-identification
8. Right to Request Deletion
9. Data Mobility
10. Service Provider Protections

***This Advisory is not intended to be a complete statement of the law and does not constitute legal advice. As this Advisory is for information purposes only, no person should act or rely upon the information contained in this Advisory without seeking legal advice.***

---

## 1. New Oversight and Enforcement Regime

Bill C-36 amends Canada's private sector privacy laws by transferring regulatory oversight to the Digital Safety and Data Protection Commission of Canada (the "Commission") with a dedicated Privacy and Consumer Data Commissioner **(s. 85(1))** and a Privacy and Consumer Data Division (established under **s. 89**). The Commission will have the power to issue compliance orders and impose significant penalties:

- Up to $10 million or 3% of the organization's gross global revenue, whichever is greater, for standard non-compliance; **(s. 114)** and

© 2026 Deeth Williams Wall LLP

Helping Your Ideas Take Flight For Over 25 Years.

- Up to $25 million or 5% of the organization's gross global revenue, whichever is greater, for the most serious offences. (**s. 145**)

## 2. Privacy Management Program Requirements (s. 9, s.10(1), s.10(2))

An organization must implement a privacy management program to protect individuals' personal information and to fulfill its obligations under the PPCDA. On request, the organization must provide the Commission access to the policies, practices and procedures included in its privacy management program. After review, the Commission may provide guidance on the organization's privacy management program or recommend corrective measures.

## 3. Updated Consent Framework (s. 12 (3), s. 15, s. 18(1), s. 18(3))

### *A. Consent Requirements*

An organization must obtain valid consent for the collection, use, or disclosure of personal information. They must tell individuals the specific purpose for which the individual's personal information will be collected, used or disclosed, and that purpose must be recorded.

### *B. Business Activities and Legitimate Interest Exceptions*

The PPCDA includes exceptions to the consent requirements for the collection, use or disclosure of personal information. However, there are two key general exceptions to the consent requirements:

i. Organizations are authorized to collect or use personal information for a business activity without consent where a reasonable person would expect the collection or use of their information for the business activity.

ii. Organizations may collect, use or disclose personal information where the collection, use or disclosure is done for an activity in which the organization has a legitimate interest that outweighs any reasonably foreseeable adverse effects to the individual. Reliance on the legitimate interest exception imposes additional obligations on the organization including obligations to identify and describe its legitimate interest in the proposed activity, conduct a privacy impact assessment, and implement risk mitigation measures.

These exceptions do not apply where the collection or use or the collection, use or disclosure, as applicable, is for the purpose of influencing the individual's behaviour or decisions.

## 4. Cross-Border Information Transfer Requirements (s. 57)

Before disclosing or transferring personal information outside Canada, an organization must conduct a privacy impact assessment and implement measures to mitigate the risks identified in

© 2026 Deeth Williams Wall LLP

the privacy impact assessment. On request, the organization must provide the Commission with access to or a copy of the privacy impact assessment.

### 5. Automated Decision System Requirements (s. 63(4)-(5))

Automated decision systems include any technology that assists or replaces human judgment through the use of rules-based systems, machine learning or other techniques.

When an organization uses an automated decision system to make a prediction, recommendation, or decision about an individual that could have a legal or similarly significant effect, on request of the individual, the organization must provide an explanation, including the type of personal information used, its source, and the principal factors involved.

### 6. Enhanced Privacy Safeguards for Children (s. 2(1), s. 9(2), s. 56(1))

A child's personal information is treated as "sensitive" information requiring organizations to apply enhanced safeguards and stricter handling requirements. The enhanced safeguards include implementing physical, organizational, and technological security controls that are strictly proportionate to the sensitive nature of the data.

### 7. Anonymization and De-identification (s. 2(1), s. 6(5), s. 20, s.75)

Anonymized information and de-identified information are differentiated from each other in Bill C-36. Anonymization permanently modifies personal information so that there is no reasonably foreseeable risk of identifying an individual, whereas de-identification modifies personal information so that an individual cannot be directly identified from it. (Anonymization and de-identification definitions are new to the federal private sector privacy regime and were not present under PIPEDA.)

Anonymized information falls outside the scope of the Act, while de-identified information remains subject to it. An organization is not required to obtain the consent of an individual to anonymize or de-identify the individual's personal information.

### 8. Right to Request Deletion (s. 54 (1))

An individual has the right to request the deletion of their personal information that is under the organization's control.

### 9. Data Mobility (s. 72, s. 140(a))

An individual has the right to request a transfer of their data directly from one organization to another. Regulations may require safeguards to ensure secure disclosure and collection of personal information between organizations.

© 2026 Deeth Williams Wall LLP

### 10. Service Provider Protections (s. 2(1), s. 11(1), s. 11(2), s. 56, s. 61)

A service provider provides services for or on behalf of another organization to assist it in fulfilling its purposes. An organization transferring personal information to a service provider must ensure the service provider provides a level of protection of the personal information equivalent to that which the organization is required to provide. The service provider's obligations, as service provider, are limited to the obligation to protect personal information through physical, organization and technological security safeguards and to notify the organization of security breaches. However, if the service provider collects, uses, or discloses the information for purposes beyond those for which it was transferred to the service provider, it is subject to the full set of obligations.

## Conclusion

Organization should, as soon as possible, begin to update (or develop) policies that will be affected by the coming into force of the PPCDA. As a first step towards compliance with the PPCDA, your organization may wish to review the issues that are identified in this Advisory.

© 2026 Deeth Williams Wall LLP

Helping Your Ideas Take Flight For Over 25 Years.