Canada privacy laws: What U.S. businesses need to know

March 10, 2026

If you are a consumer-facing business in the United States or are in the field of advising them on privacy matters, you are aware of the importance of privacy and data protection compliance.

Despite this awareness, too many companies and counsels tend to overlook the need to consider Canadian privacy laws, especially when engaging in cross-border commercial transactions, and overlooking at the same time Québec privacy law which has a strict regime comparable to the GDPR, with fines reaching up to $25 million or 4 per cent of global revenue.

To assume that U.S. and Canadian privacy laws are the same would be misleading. This page offers guidance on how U.S. businesses can navigate Canadian privacy laws. It provides an overview of Canadian privacy legislation, highlights key elements, and concludes with practical considerations to keep top of mind prior to engaging in and during commercial transactions.

Overview – Canada's privacy laws

Canadian privacy laws do not contain residency restrictions, they apply regardless of the nationality of the individuals when their personal information is processed in Canada, but also regardless of where the data processing occurs – even outside Canada - when personal information of Canadians is processed. As such, U.S. organizations that process Canadian personal information may be subject to both U.S. and Canadian privacy laws.

Canada has a comprehensive federal privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA governs how private sector organizations collect, use, and disclose personal information about individuals in the course of commercial activities.

PIPEDA applies across Canada, except in provinces that have enacted privacy laws deemed "substantially similar", notably Alberta (*Personal Information Protection Act*), British Columbia (*Personal Information Protection* Act), and Québec (*Act respecting the protection of personal information in the private sector*) – see BLG guide on Québec

private sector Act here for more information. PIPEDA also applies to organizations that transfer personal information across provincial or international borders.

While the privacy laws in the provinces of Alberta and British Columbia are akin to PIPEDA, the privacy laws in the province of Québec are frequently compared to the *European General Data Protection Regulation* (GDPR) given its strong alignment with the regulation, including in terms of sanctions.

Last, in the employment context, PIPEDA applies only to federally regulated industries, such as banking, airlines, and railways.

Key elements of Canada's privacy laws

1 – Consent

Canadian privacy laws are built around the principles of transparency and consent. Before collecting, using or disclosing personal information, organizations must ensure individuals understand and agree to the specific purposes for which their data will be used. Consent must be meaningful and clearly communicated in plain language. The form of consent, express or implied, depends mainly on the sensitivity of the information and the context.

That being said, Canadian privacy laws, depending on the province, may provide exceptions to these consent requirements in certain situations such as in an employment context, during a commercial transaction or a business context. These various exceptions highlight the need for businesses to tailor their privacy practices to the province with which they are dealing.

2 – Limitations

U.S. businesses operating in Canada must understand that indiscriminate data collection is not permitted. Canadian privacy laws mandate data minimization, meaning organizations may only collect personal information that is necessary for the identified purpose. Both the amount and type of data must be limited accordingly. Additionally, organizations are required to implement retention policies that ensure personal information is only kept for as long as needed to fulfill its purpose. Once the purpose is met, the data must be destroyed, erased or anonymized, unless retention is required by law.

Canadian privacy laws impose a reasonableness standard that applies regardless of consent. Organizations may only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate under the circumstances. Privacy regulators apply a four-part test to assess this, notably whether: (1) the organization's purpose represents a legitimate need/*bona fide* business interest, (2) the process would be effective in meeting this need, (3) there aren't any less-invasive ways to achieve the same ends at comparable cost and with comparable benefits, and (4) the loss of privacy is proportional to the benefits. This element adds a layer of accountability that goes beyond consent, ensuring that an organization's privacy practices are not only lawful, but also minimal and reasonable.

3 – Cross-border transfers

While Canadian laws are not as stringent as the GDPR in this area, U.S. businesses must still be aware of the requirements they must meet before transferring personal information of Canadian customers or employees to the United States.

At the federal level, PIPEDA requires organizations to remain responsible for personal information that has been transferred to a third party for processing, including those located outside Canada. PIPEDA requires organizations to use contractual or other means to ensure a comparable level of protection while the data is being processed. As well, the Office of the Privacy Commissioner's (OPC) federal guideline explains that, in accordance with the obligation of transparency, organizations must notify the individuals concerned that information is being transferred outside Canada along with the fact that there is a risk foreign authorities may access it.

In Québec, the provincial law explicitly states the requirement of organizations to inform the person concerned of the possibility that the information could be communicated outside Québec and requires organizations to conduct a privacy impact assessment (PIA). The transfer may only proceed if the PIA concludes that the information will receive adequate protection considering the generally-recognized principles regarding the protection of personal information. Furthermore, a written contract is also required to govern the transfer, which is discussed further below in Section 6 – Data Processing Agreements. For more detailed guidance, we invite you to consult BLG's bulletin on cross-border transfers.

4 – Breaches

U.S. businesses should be aware of Canada's breach notification obligations. Canadian privacy laws require organizations to report to the competent privacy regulator and notify the individual (and any other organization it believes may be able to mitigate harm) of any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm/risk of serious injury to the individual. Organizations must take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature. Organizations shall also keep and maintain a record of every breach that has occurred under its control, in accordance with specific regulatory requirements.

5 – Biometrics

With the rise of technologies like facial recognition and voice analysis, privacy regulators have begun to address the unique risks posed by biometric data. At the federal level in Canada, the OPC recently issued a new guidance on protecting privacy in biometric initiatives. The OPC guidance for private-sector organizations provides information on privacy obligations under PIPEDA and best practices for processing biometric information, such as identifying an appropriate purpose, obtaining consent, limiting its collection, use, disclosure, and retention, and issuing appropriate safeguards. BLG has analysed this guidance for you here.

While U.S. businesses should certainly read and comprehend the guidance, it is, nonetheless, their responsibility to ensure they understand all their obligations under

applicable laws and regulations that apply to them. For example, privacy laws in Québec impose additional and stricter obligations with respect to biometric information. Organizations wishing to use biometrics are required to disclose this fact to the Commission d'accès à l'information (CAI) prior to implementation if they: (1) verify or confirm the identity using a process that captures biometric characteristics, and/or (2) create a database of biometric characteristics or measurements, in which case, disclosure must be made at least 60 days before the database is put into service.

6 – Data processing agreements

U.S. businesses operating in Canada should be aware of a common legal requirement when contracting with third party service providers involving personal information: the need for a data processing agreement (DPA). When a business engages a third party to process personal information on their behalf, Canadian privacy laws require that a DPA be in place. This agreement, either as a standalone contract or an addendum, ensures that service provider processes personal data in compliance with applicable privacy legislation.

Under PIPEDA, organizations remain responsible for personal information in their possession or custody, even when it is transferred to a third party for processing. To meet this obligation, organizations must use contractual means to ensure a comparable level of protection while the data is being processed. A DPA helps clarify the roles and responsibilities of both parties.

In Québec, DPAs are especially critical as these fall under one of the exceptions to obtaining consent, subject to specific legal requirements. The law requires that a DPA be made in writing and specify certain requirements such as: (1) the measures that the processor must take to protect the confidentiality of the personal information communicated, (2) a prohibition on using the data for any purpose other than fulfilling the contract and a requirement to delete it after the contract ends, (3) an obligation to notify the disclosing party without delay of any violation or attempted violation by any person of any obligation concerning confidentiality, and (4) the disclosing party's right to conduct any verification relating to confidentiality requirements.

7 – Privacy-by-default

Depending on how a business intends to collect personal information, it should be aware of certain default privacy settings required under Canadian privacy laws, particularly in Québec, though similar principles are reflected in federal reports under PIPEDA.

Québec's privacy law states that an organization that collects personal information using technology that includes functions allowing the person concerned to be identified, located or profiled must first inform the person of the use of such technology and, more importantly, of the means available to activate the functions that allow for such features. The term "profiling" includes the analyzing of a person's work performance, economic situation, and health. This means that such functions must be deactivated by default, requiring users to take an affirmative action to signify their agreement to activate those functions. While PIPEDA does not contain an equivalent provision, the OPC has emphasized that technologies involving sensitive information such as precise location typically require express (opt-in) consent under their general consent rules.

In addition, under Québec's privacy laws, an organization that collects personal information when offering to the public a technological product or service having privacy settings must ensure that those settings provide the highest level of confidentiality by default, without any intervention by the person concerned. This rule does not apply to privacy settings for browser cookies. Although PIPEDA does not contain a specific provision on default settings, the OPC has taken the position that these settings should be set in accordance with the reasonable expectations of individuals.

8 – Enforcement

U.S. businesses should be aware of Canada's privacy enforcement structure. At the federal level, the OPC oversees compliance with PIPEDA. The OPC has the authority to investigate complaints, conduct audits, and issue reports containing non-binding recommendations. It can also enter into compliance agreements with organizations to encourage corrective action. However, the OPC's enforcement powers are limited in that they cannot issue direct fines or binding orders. To enforce its findings, the matter must be brought before the Federal Court, either by the OPC or the complainant.

By contrast, provincial regulators have more robust enforcement powers. In Québec, the CAI has all the powers necessary for the exercise of its jurisdiction, which includes making an order it considers appropriate to protect the rights of the parties. There are three types of sanctions that the CAI can impose, notably: (1) an administrative monetary penalty of up to $10 million or 2 per cent of global turnover, (2) a penal penalty of up to $25 million or 4 per cent of global turnover, and (3) punitive damages of no less than $1,000 when the violation is intentional or results from gross fault.

In addition to privacy-specific regulators, the Competition Bureau of Canada plays a complementary role in privacy enforcement where privacy intersects with consumer protection and deceptive marketing practices. For instance, the Bureau in 2020 concluded its first privacy-related settlement with Facebook in which it agreed to pay a $9 million penalty for making false and misleading claims about the privacy of Canadians' personal information on Facebook and Messenger.

Practical considerations and obligations for commercial transactions

This section outlines the practical considerations and obligations for U.S. businesses during commercial transactions in Canada. As a final note, we highlight four essential privacy and data protection elements to keep top of mind.

1 – NDAs require specific customization

Standard non-disclosure agreements (NDAs) may not meet the legal requirements in provinces like Québec where the law mandates specific language to protect personal information during a transaction. As generic templates often fall short of compliance, legal counsel familiar with the province's privacy regime should review and tailor NDAs to ensure they reflect legislative obligations.

2 – Privacy due diligence is critical

During the due diligence phase of a transaction, it is essential to identify and assess specific legal privacy requirements. Even if a target organization may have a robust privacy framework, including detailed policies and procedures governing the processing of personal information from customers and employees, a thorough risk and gap analysis based on applicable provincial laws and regulatory guidance must be conducted by local counsel. This review may reveal compliance issues that can either be remediated post-closing or justify the inclusion of additional indemnity provisions in the share or asset purchase agreement.

3 – Post-closing notification obligations

Following a transaction, the acquiring entity may be required to notify affected individuals of changes in the possession or control of their personal information. Notifications must clearly inform individuals of the nature of the change, the new entity's identity, and how their personal information will be used going forward. This may even trigger a requirement to obtain new informed consent if the purpose differs from those originally disclosed. Local legal advisors play a key role in crafting these communications to ensure they are tailored to the specific groups affected, written in plain language, and compliant with applicable provincial and federal obligations.

4 – Ongoing privacy management post-transaction

After closing, the new entity must promptly address any privacy risks identified during the due diligence process to avoid penalties and reputational damage. The new entity must establish an ongoing privacy management process, including proper training for its privacy officer and all personnel who process personal information. A local lawyer can provide ready-to-use templates and can help adapt existing policies and processes to ensure optimal compliance.

BLG can help

We hope that this article, including the four key privacy points, are carefully considered during your company's next commercial transaction in Canada.

For tailored guidance, please reach out to BLG's privacy team. We are here to help you navigate the evolving legal landscape.

By

Hélène Deschamps Marquis, Candice Hévin, Abby Shine

Expertise

Compliance with Privacy & Data Protection, United States

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.