Canada: Privacy Law Overview

Stikeman Elliott LLP

Stikeman Elliott

Canada: Privacy Law Overview

General 2

Private Sector Privacy Laws 2

- Oversight and Enforcement 3
- Key Obligations and Restrictions 4

Health Sector Privacy Laws 6

Public Sector Privacy Laws 7

Outsourcing and Data Transfers 8

This is Section O of *Doing Business in Canada*, published by Stikeman Elliott.

Canada: Privacy Law Overview

General

Privacy and data protection requirements in Canada may originate from a number of different sources, depending on factors such as the industrial sector in which an organization operates, the jurisdiction in which that organization is located, and the jurisdiction from which personal information was collected or is held or processed by that organization.

Since Canada is a federal state, its legal framework for privacy can be somewhat complex. Statutes exist at both the federal and provincial level, a consequence of a complex constitutional division of powers in this area that includes certain areas of overlap between the two levels of government. The privacy law framework is also complicated by the fact that in many Canadian provinces, there are distinct statutes governing private sector organizations, public sector organizations and health sector organizations. Unique legal issues also arise with respect to employee privacy.

In addition, there are a number of sector-specific laws that incorporate requirements respecting the collection, use and storage of personal information. Examples include laws respecting transportation and telecommunications, laws respecting credit reporting agencies and laws relating to law enforcement and national security agencies.

Private Sector Privacy Laws

Of chief interest to business are the four generally-applicable privacy and data protection statutes in Canada that govern the private sector. Three of these are provincial statutes while the fourth is federal:

- **Alberta:** *The Personal Information Protection Act* (AB PIPA)
- **British Columbia:** *The Personal Information Protection Act* (BC PIPA)
- **Québec:** *An Act respecting the protection of personal information in the private sector* (APPIPS)
- **Federal:** *The Personal Information Protection and Electronic Documents Act* (PIPEDA)

Each of the provincial private sector laws applies generally within the province in question, governing all private sector activities within that province that involve the collection, use and disclosure of personal information, including the handling of personal information by non-profit organizations and by both national and international businesses. These laws also cover employee privacy.

The federal law, PIPEDA, applies to organizations subject to federal regulation, to inter-provincial and international transactions involving personal information in the course of commercial activities, and to commercial organizations operating wholly in a province that has not enacted its own private sector privacy legislation. However, in employment contexts, PIPEDA applies only to the employees of the relatively small number of industries that fall under federal jurisdiction (such as airlines, banks, broadcasters, railroads and telecommunications carriers). As a result, in those provinces without their own private sector privacy law, there is no privacy legislation applicable to the personal information of most employees.

One area of apparent and unresolved overlap between the federal and provincial private sector privacy laws relates to inter-provincial and international transfers of personal information. PIPEDA declares that it applies to all such transfers, yet the provincial laws also contain provisions respecting out-of-jurisdiction transfers, including, variously, requirements relating to such matters as notice to individuals, pre-transfer impact assessments and measures to protect personal information transferred outside of Canada (or, in the case of Québec, outside that province).

Oversight and Enforcement

A privacy authority for each of the above jurisdictions (Alberta, British Columbia, Québec and the federal jurisdiction) oversees the application and enforcement of the applicable private sector privacy law:

- **Alberta:** The Information and Privacy Commissioner of Alberta
- **British Columbia:** The Information and Privacy Commissioner for British Columbia
- **Québec:** The *Commission d'accès à l'information*
- **Federal:** The Privacy Commissioner of Canada

The roles and powers of these authorities vary considerably. The Privacy Commissioner of Canada, who enforces the federal law, generally functions on an ombudsman model, investigating complaints and making recommendations, but with no direct order-making or enforcement powers. Although the Commissioner lacks direct remedial order making powers, they can bring applications to the Federal Court to hear a matter considered by their office, and the court can award damages and issue mandatory and injunctive orders.

By contrast, the Information and Privacy Commissioners for each of Alberta and British Columbia also have the power to issue mandatory and injunctive orders, including, in the case of Alberta, the power to make orders with respect to notifications to be provided to affected parties in the case of a data breach.

The *Commission d'accès à l'information* has powers similar to those of its provincial counterparts, and, commencing in September 2023, will have also have the power to impose significant monetary penalties for violations of the Québec law: up to $10 million or 2% of the company's global turnover.

Failure to adhere to specified obligations or prohibitions under private sector privacy laws also constitute offences, which may be prosecuted by the Attorney General for the applicable federal or provincial jurisdiction. For example, a failure to report an incident or a breach to the appropriate Commissioner constitutes an offence under the federal, Alberta and Québec laws. Similarly, a failure to comply with an order of a provincial privacy commissioner may also constitute an offence. In Québec, most violations of the requirements of the private sector privacy law can constitute an offence. The fines that may be imposed for violations of these privacy laws vary between jurisdictions: in some cases, the maximum penalties for a first offence are generally below $10,000, while violations of some provisions of PIPEDA can result in fines of up to $100,000. Commencing in September 2023, businesses that violate Québec's private sector privacy law can be fined up to $25 million or 4% of global turnover, whichever is greater.

Key Obligations and Restrictions

Canadian private sector privacy laws are based on the same OECD principles that underlie laws like the European General Data Protection Regulation (GDPR), so Canadian private sector privacy laws contain similar obligations and restrictions to many international data protection frameworks. In fact, under the predecessor to the GDPR, the EU formerly recognized PIPEDA as providing an adequate level of data protection, meaning that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to an organization subject to PIPEDA without any further safeguard being necessary.[1] Following Brexit, this "adequacy" finding was also extended to apply to transfers from the United Kingdom under the UK GDPR.

Because Canadian privacy laws tend to be principles-based, they generally afford organizations more flexibility than the more prescriptive privacy laws that exist in some other jurisdictions, while still covering much of the same subject matter and granting similar individual rights.

Focus of Laws

Each of the Canadian private sector privacy laws imposes obligations on organizations with respect to the collection, use and disclosure of "Personal Information," which is defined to mean information about an identifiable individual, but does not include certain business contact information, such as the name, title or business address or telephone number of an employee of an organization.

---

[1] Decisions adopted by the European Commission on the basis of Article 25(6) of Directive 95/46/EC remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with the adequacy provisions of the GDPR.

Since personal information must be about an identifiable individual, aggregated and anonymous data is not considered to be personal information; however, Canadian courts have held that information will be about an "identifiable individual" where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information. Québec's privacy law requires organizations to take reasonable measures to limit the risk that someone will identify a natural person using de-identified information, and prohibits anyone from identifying or attempting to identify a natural person using de-identified information.

Private sector privacy laws focus on the organization that ultimately controls the collection and processing of personal information, and such controlling organizations remain responsible at law for the appropriate treatment of that information, including where it has been transferred to a third party for processing (for more on outsourcing, see below.)

Consent

At their essence, Canadian private sector privacy laws require the knowledge and consent of the individual concerned for any collection, use and disclosure of personal information. Consent may be implicit or explicit, depending on the circumstances. Factors to be considered in determining the appropriate form of consent include the inherent sensitivity of the information and the reasonable expectations of the individual. Organizations must make reasonable efforts to ensure that the individual is advised of the purposes for which the consent may be used. To be meaningful, the purposes must be stated in a reasonably understandable manner. Consent cannot be required as a condition of the supply of a product or service, unless the consent relates to legitimate purposes that are directly related to the transaction. For example, consent to secondary marketing cannot be made a condition of the provision of a product or service. It is a requirement that consent can be withdrawn at any time.

Canadian privacy laws tend not to be particularly prescriptive with respect to permitted purposes for the collection, use and disclosure of personal information; however, any such purposes must be objectively reasonable, even in cases where express consent has been obtained.

There are a number of explicit statutory exceptions to the requirement for consent with respect to the collection, use and disclosure of personal information. For example, among other exceptions, collection is permitted without consent where it is reasonable to expect that collection with consent would compromise the availability or accuracy of the information, and the collection is reasonable for purposes relating to breach of a law. In addition, personal information may be disclosed without consent in certain cases, such as for the purpose of collecting a debt owned by the individual to the organization, or where disclosure is required to comply with a subpoena, warrant or order issued by a court or other body with jurisdiction to compel the production of information. While there are a number of

such statutory exceptions, varying somewhat between jurisdictions, Canadian private sector privacy laws do not contain equivalents to the broad alternate grounds for processing contained in the GDPR, such as "legitimate interests" or "required to fulfill a contract".

The law also recognizes that personal information may be transferred to third parties for processing (without consent, or based on implied consent); however, the organization transferring the data remains responsible for compliance with privacy and data protection requirements (for more on outsourcing, see below.)

Minimization, Safeguarding & Breach Reporting

Canadian private sector privacy laws also require that personal information be collected, used, disclosed and retained only as necessary to fulfill the purposes for which it was collected and for which consent, where applicable, was obtained. Personal information cannot be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law, and must be retained only as long as necessary for the identified purposes. Access to personal information within an organization should be limited to employees with a clear need-to-know based on their job function.

Canadian privacy laws are not particularly prescriptive with respect to data security obligations, instead imposing a general obligation to protect personal information by security safeguards appropriate to the sensitivity of the information in question. The methods of protection are to include physical, organizational and technological measures and should safeguard the personal information in question against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. The adequacy of security measures implemented by an organization is often assessed by privacy commissioners with respect to implementation of recognized third-party certifications and standards, as well as by comparison with perceived prevailing security practices within the relevant industrial sector.

Mandatory breach reporting/notification is required under PIPEDA, as well as under the private sector laws of Alberta and Québec, where there has been unauthorized access to, or use, disclosure or loss of personal information. Reporting to the relevant privacy authority, or notification to an affected individual, is required when the breach incident gives rise to a risk of serious harm.

Health Sector Privacy Laws

All but two provinces have their own privacy statute governing the health services sector; however, health information privacy in the provinces of British Columbia and Québec is governed by the public sector laws in those provinces. Health sector laws are supervised and enforced by a designated information and privacy commissioner in each of the relevant provinces.

Health sector privacy laws vary slightly from province to province, but generally apply to healthcare providers, such as:

- licensed healthcare professionals;
- hospitals;
- clinics;
- laboratories; and
- long-term care facilities.

Health sector privacy laws govern the collection and processing of "personal health information", a subset of personal information that relates to the physical or mental health of an individual, including the provision of treatment and eligibility for healthcare coverage.

Under health sector privacy laws, consent is generally not required in order to use personal health information for the provision of healthcare services, including within the "circle of care". However, explicit consent is required for certain additional uses and for disclosure to third parties to be used for those parties' own purposes.

Public sector laws can also apply to certain activities of healthcare institutions, given that the healthcare system is largely publicly funded in Canada.

For the most part, health information privacy laws do not apply directly to suppliers and service providers to health care providers, although such businesses should expect that health care provider customers will want to impose contractual obligations and restrictions on suppliers to ensure that those customers will be able to meet their statutory obligations under the health sector laws. Notably, several of the health information privacy laws do impose direct restrictions and obligations on service providers to health care providers requiring, variously, that such providers use personal health information solely to provide the service in question, keep that information confidential, restrict access by the supplier's employees to a need-to-know basis, protect the information using appropriate safeguards and notify promptly the health care provider in the event of any unauthorized access, use, disclosure or disposal of personal health information.

Public Sector Privacy Laws

Each province also has its own privacy statute governing public sector organizations. In addition to governing the protection of personal information in the public sector, the public sector privacy laws generally also serve as freedom of information statutes.[2] Public sector laws are supervised and enforced by the

[2] Federally, freedom of information is governed by the A*ccess to Information Act*, a separate statute from the public sector privacy law, the *Privacy Act*.

designated information and privacy commissioner in each of these jurisdictions, or in the case of Québec, by the *Commission d'accès à l'information.*

Public sector laws apply to federal, provincial and municipal governments and agencies, as well as some Crown corporations (as certain arm's-length government-owned enterprises are known in Canada). They also generally apply to municipalities, public schools and school boards, public universities/colleges and public hospitals. Public sector laws can also apply to certain activities of healthcare institutions, given that the healthcare system is largely publicly funded in Canada.

Unlike the consent-based private sector privacy laws, consent is not required for most uses of personal information by governments, although consent is required in some jurisdictions for certain extraordinary uses and disclosures, such as cross-border transfers.

Public sector privacy laws do not apply directly to suppliers and service providers to public institutions, although such businesses should expect that public sector customers will want to impose contractual obligations and restrictions on suppliers to ensure that those customers will be able to meet their statutory obligations under the public sector laws. Businesses should also be aware that any information that they provide to a public sector entity is subject to a general right of public access to records under the control of a government institution, subject to certain limited exceptions (such as trade secrets and confidential financial, commercial, scientific or technical information).

Outsourcing and Data Transfers

Under Canadian privacy laws, organizations remain responsible for the appropriate handling of personal information under their custody or control, even where such information has been transferred to third parties for processing, such as in an outsourcing arrangement. In such cases, organizations are required to use contractual and other means to provide a comparable level of protection while the information is in the hands of the third party. Privacy commissioners require outsourcing organizations to select vendors with care, to bind them contractually to use transferred personal information only for the intended purposes, to keep it confidential, and to protect it with appropriate security safeguards. Periodic audits of the third party and privacy training of third-party personnel are also required in some circumstances.

With a few exceptions, private, public and health sector privacy laws generally permit the storage or processing of personal information outside of Canada, provided that notice has been provided or consent obtained.

For private sector transfers of information, in many cases it is permissible to rely on implied consent for such purposes, such as by posting a notice or including a disclosure in an organization's privacy policy indicating that personal information may be transferred outside the country, where it will be subject to the local laws in

the jurisdiction in which it resides. Commencing September 2023, before transferring information outside of Québec, or engaging a firm to collect personal information outside that province on its behalf, Québec's private sector law will require organizations to conduct a privacy impact assessment that demonstrates that the personal information will receive adequate protection in the hands of the processor.

Health sector statutes also generally allow for transfers of personal health information outside of Canada where necessary for the provision of healthcare services, but require individual consent for cross-border transfers in other circumstances.

Similar to the Québec private sector law, the public sector privacy law in British Columbia requires that a public body must conduct a privacy impact assessment before transferring personal information under its control outside of Canada. In Nova Scotia, it is generally prohibited to transfer outside of Canada any personal information under the control of public bodies in that province, subject to the approval of the head of the governmental body that proposes to conduct the transfer, or to other narrowly defined exceptions.

Finally, it should also be noted that several sector-specific laws, such as federal laws respecting banking and taxation, require that certain records be retained in Canada.

About the Firm

When Heward Stikeman and Fraser Elliott first opened the firm's doors in 1952, they were united in their pledge to do things differently to help clients meet their business objectives.

In fact, they made it their mission to deliver only the highest quality counsel as well as the most efficient and innovative services in order to steadily advance client goals.

Stikeman Elliott's leadership, prominence and recognition have continued to grow both in Canada and around the globe. However, we have remained true to our core values.

These values are what guide us every day and they include:

- Partnering with clients – mutual goals ensure mutual success.
- Finding original solutions where others can't – but they must also be grounded in business realities.
- Providing clients with a deep bench of legal expertise – for clear, proactive counsel.
- Remaining passionate about what we do – we relish the process and the performance that results from teamwork.

A commitment to the pursuit of excellence – today, tomorrow and in the decades to come – is what distinguishes Stikeman Elliott when it comes to forging a workable path through complex issues. Our duty and dedication never waver.

This is what makes Stikeman Elliott the firm the world comes to when it counts the most.

Montréal

1155 René-Lévesque Blvd. W.
41st Floor
Montréal, QC, Canada H3B 3V2
Tel: 514 397 3000

Toronto

5300 Commerce Court West
199 Bay Street
Toronto, ON, Canada M5L 1B9
Tel: 416 869 5500

Ottawa

Suite 1600
50 O'Connor Street
Ottawa, ON, Canada K1P 6L2
Tel: 613 234 4555

Calgary

4300 Bankers Hall West
888 – 3rd Street S.W.
Calgary, AB, Canada T2P 5C5
Tel: 403 266 9000

Vancouver

Suite 1700, Park Place
666 Burrard Street
Vancouver, BC, Canada V6C 2X8
Tel: 604 631 1300

New York

845 Third Avenue, 20th Floor
New York, NY USA 10022
Tel: 212 371 8855

London

36 Cornhill
London EC3V 3NG
Tel: 44 (0) 20 7367 0150

Sydney

Level 24
Three International Towers
300 Barangaroo Avenue
Sydney, NSW 2000
Tel: +61 (2) 8067 8578

Follow us

SE

Stikeman Elliott

Subscribe to updates on a variety of valuable legal topics from Stikeman Elliott's Knowledge Hub.