



7. Privacy and Anti-Spam Laws

Privacy Law

The protection of personal information in Canada is governed by the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and by substantially similar legislation in certain provincial jurisdictions.

PIPEDA

Defining Personal Information

Personal information is broadly defined in PIPEDA as “information about an identifiable individual.” Such information can include, among other things, a person’s name, address, phone number, age, sex, ethnicity, religion, education, and health and financial information. Certain government-provided information is also considered personal, such as a person’s social insurance number, provincial health insurance plan number, driver’s licence number, and passport number.

Application of PIPEDA

In general terms, PIPEDA applies to an organization’s collection, use, or disclosure of personal information in the course of commercial activities. It also applies to the personal information of employees when it is collected, used, or disclosed in connection with the operation of a federal work, undertaking, or business.

PIPEDA does not apply to the collection, use, or disclosure of employees’ personal information where individuals are employees of organizations under provincial jurisdiction (i.e. organizations that are not federal works, undertakings, or businesses). However, the private sector privacy legislation in British Columbia, Alberta, and Québec does apply to employees’ personal information. Consideration must also be given to other statutory and common law sources of privacy law obligations in the workplace and in certain industry sectors (e.g. health care in respect of personal health information).

The general principles of PIPEDA are:

- Accountability
- Identifying purposes
- Consent
- Limiting collection
- Limiting use, disclosure, and retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance

PIPEDA and Your Business

Knowledge and Consent

Informed consent is the guiding principle behind PIPEDA. Individuals should be made aware of the purposes for the collection, use, or disclosure of their personal information, and they should have the right to either consent to or refuse such action. Consent is valid only if it is reasonable to expect that the affected individual would understand the “nature, purpose, and consequences” of the collection, use, or disclosure of the personal information to which he or she is granting access.

There are certain exceptions to the consent requirement. For example, there is a consent exemption available for information collection where such collection is for the benefit of the individual in question and consent cannot be obtained in a timely way or where the information is “publicly available” (the scope of which is narrowly prescribed by the regulation).

Business Transactions

It is often necessary for organizations to collect, use, or disclose personal information, including employees’ personal information, in relation to due diligence and closing a business transaction. PIPEDA permits these activities without consent, provided that the organization has entered into an agreement that requires the recipient to (i) use the information for the sole purpose of the transaction, (ii) protect the information, or (iii) return or destroy the information if the transaction does not proceed.

For completed transactions, the organization must enter into an agreement that requires it to (i) use and disclose the information for the sole purposes for which it was collected, used, or disclosed prior to the transaction; (ii) protect the information; and (iii) give effect to any withdrawal of consent.

The information must be necessary for carrying on the activity that was the object of the transaction, and one of the parties must notify the individuals within a reasonable time of the transaction and disclosure.

The above exemption does not apply if the transaction is for the primary purpose of, or results in, the purchase (or other acquisition), sale, disposition, or lease of personal information. The exemption codifies common practice and is modelled on similar provisions in British Columbia and Alberta privacy laws.

Outsourcing of Data Processing to the United States

Canadian corporations may outsource certain data processing activities, like client billing, to an American parent corporation or a third-party processing company located within the United States or another jurisdiction. Although PIPEDA does not prohibit the outsourcing of data processing activities, it does require that the Canadian organization continues to be accountable for the personal information even though such information has been transferred to a third party for processing.

In addition, the Canadian organization will have to comply with two requirements imposed by the Office of the Privacy Commissioner of Canada (the commissioner). First, as with all third-party processing (whether it takes place in or outside of Canada), the organization must protect the confidentiality and security of the personal information through either (i) implementing adequate contractual and other safeguards between the organization and the parent corporation (or third-party processor) or (ii) ensuring that the subsidiary and parent corporations are governed by the same privacy policy that imposes the same privacy requirements on both entities. Second, the Canadian subsidiary must notify the affected

individuals if their personal information will be stored, used, or disclosed in a jurisdiction outside of Canada and that the information may be accessible under the laws of the relevant jurisdiction. Additional requirements may be applicable in respect of certain types of information and pursuant to provincial privacy laws.

Breach Notification and Record Keeping

Pursuant to provisions that came into effect on November 1, 2018, PIPEDA includes a mandatory requirement for organizations to give notice to affected individuals and to the commissioner about data breaches under certain circumstances.

Section 10.1 of PIPEDA requires organizations to notify individuals about (unless prohibited by law), and to report to the commissioner, all breaches where it is reasonable to believe that the breach creates a “real risk of significant harm to an individual.”

PIPEDA defines “significant harm” as including, among other harms, humiliation, damage to an individual’s reputation or relationships, and identity theft. A “real risk” requires consideration of the sensitivity of the information, the probability of misuse, and any other prescribed factor.

The notice to individuals and the report to the commissioner must be given in the prescribed form “as soon as is feasible” after it is determined that a breach occurred. The commissioner may publish information about such notices if it determines that it would be in the public interest to do so.

Pursuant to the Breach of Security Safeguards Regulations under PIPEDA, the notice to an individual must contain certain information, including a description of (i) the circumstances of the breach, (ii) the personal information that is the subject of the breach, (iii) the steps taken by the organization to reduce the harm that

could result, and (iv) the steps the individual can take to reduce or mitigate the harm. The notice must be conspicuous and given directly to the individual except in certain circumstances where indirect notice may be permitted (e.g. posting to a website).

The report to the commissioner must contain certain information, including the number of individuals affected, contact information for someone who can answer the commissioner’s questions, and a description of (i) the circumstances of the breach, (ii) the personal information that is the subject of the breach, (iii) the steps taken by the organization to reduce the harm that could result, and (iv) the steps the organization has taken to notify the affected individuals. The report may be sent by “any secure means of communication” and may be updated with new information as the organization becomes aware of it.

Where notice is given to individuals, section 10.2 of PIPEDA requires organizations to notify other organizations (e.g. credit bureaus) and government agencies if such notice could reduce the risks or mitigate the harm. Consent is not required for such disclosures.

Section 10.3 of PIPEDA requires organizations, in accordance with the prescribed requirements, to keep and maintain a record of every breach of safeguards involving personal information under their control. Pursuant to section 6 of the Breach of Security Safeguards Regulations, these records must be maintained for twenty-four months after the day on which the organization determines the breach happened. The records must also contain the information necessary to allow the commissioner to verify compliance with the reporting and notification requirements under section 10.1 of PIPEDA.

In addition, upon request, organizations must provide the commissioner with such records. The commissioner may publish information from such records if it would be in the public interest.

There is no threshold associated with the record-keeping obligation; a record of all breaches of security safeguards must be kept, irrespective of whether or not they gave rise to a real risk of significant harm. Nor is there any threshold before an organization would be required to provide its “breach file” to the commissioner.

Provincial Legislation

The provinces of Québec, Alberta, and British Columbia have enacted privacy legislation that is substantially similar to PIPEDA, although it is not limited to organizations’ commercial activities. As a result, the provincial legislation may apply to the collection, use, or disclosure of personal information within those jurisdictions.

Anti-Spam Law

Sending commercial electronic messages (CEMs) to and from Canada and installing computer programs on systems in Canada is primarily governed by a statute commonly known as Canada’s Anti-Spam Law (CASL) and the regulations pursuant to it.

On July 1, 2014, most of CASL and its regulations came into force. The balance of the law came into force in January 2015 (with the exception of a section on the private right of action to sue for a violation of CASL, whose scheduled commencement in 2017 was suspended).

CEMs

A CEM is defined broadly in CASL as “an electronic message that, having regard to the content of the message, the hyperlinks in the message to content on a website or other database, or the contact information contained in the message, it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity, including

an electronic message that (a) offers to purchase, sell, barter, or lease a product, goods, a service, land, or an interest or right in land; (b) offers to provide a business, investment, or gaming opportunity; (c) advertises or promotes anything referred to in paragraph (a) or (b); or (d) promotes a person, including the public image of a person, as being a person who does anything referred to in any of paragraphs (a) to (c) or who intends to do so.”

Requests for permission to send CEMs are also deemed to be CEMs, so organizations must carefully consider CASL requirements before sending a message to request consent to send CEMs.

Unlike other anti-spam laws, including the *US CAN-SPAM Act*, CASL is an opt-in regime. With limited exceptions, CASL prohibits the sending of a CEM unless prior express or implied consent exists. In addition, prescribed contact information and an unsubscribe mechanism must be included in each CEM.

Express consent must be obtained in a prescribed form under CASL. Implied consent is limited to certain enumerated categories, such as “existing business relationships” as defined in the legislation.

Computer Programs

In general terms, CASL prohibits installing or causing to be installed a computer program on any other person’s computer system or, having so installed or caused to be installed a computer program, causing an electronic message to be sent from that computer system without the express consent of the owner or an authorized user of the computer system or in accordance with a court order.

This prohibition applies if the computer system is located in Canada at the relevant time or if the person is either in Canada at the relevant time or

is acting under the direction of a person who is in Canada at the time when the direction is given.

Additional notice and consent requirements and other obligations apply in respect of programs that perform certain enumerated functions that the person who seeks express consent knows and intends will cause the computer system to operate in a manner that is contrary to the reasonable expectations of the owner or an authorized user of the computer system, such as collecting personal information stored on the computer system.

Consequences for Violations of CASL

CASL violations can lead to significant monetary penalties (up to \$10,000,000 for organizations), directors' and officers' liability, and extended liability for those involved in committing the violation.

Pursuant to the CASL regulation originally scheduled to come into force on July 1, 2017, organizations would have also faced the prospect of civil litigation (including class action litigation) and statutory damages in respect of CASL violations. The commencement of this private right of action was suspended pending further government review.