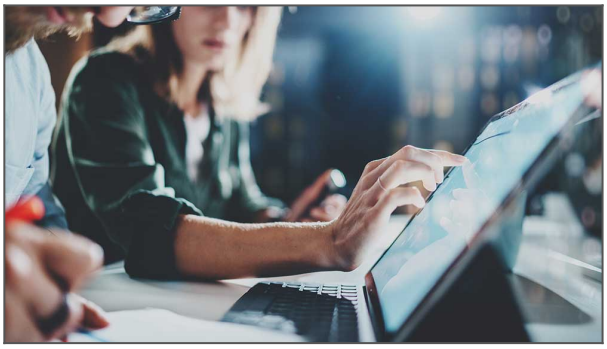
Q&A: Personal Data Handling and Processing in Canada – Updated

Authors: Doug Tait Kendall (Dell) Dyck

published 07/27/2022

Updated for 2022
This article was first written in May 2021 as part of **Lexology's Getting The Deal Through** series.



Legitimate processing of PI

Legitimate processing – grounds
Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

In general, subject to limited exceptions, Canadian private sector privacy legislation requires organisations to obtain meaningful consent for the collection, use and disclosure of PI. What constitutes 'meaningful consent' is guided by seven principles designed to ensure that the individual providing the consent has, among other things, a clear understanding of the nature, purpose and consequence of what they are consenting to, been provided information (in a clear and comprehensible manner) about the organisation's privacy management practices and been provided with a clear 'yes' or 'no' option.

Further, under the Personal Information Protection and Electronic Documents Act (PIPEDA), the purpose for which PI is collected, used or disclosed must be one that a reasonable person would consider appropriate in the circumstances. Otherwise, even with consent, the organisation will have violated PIPEDA.

Legitimate processing – types of PI
Does the law impose more stringent rules for processing specific categories and types of PI?

Privacy legislation generally states that the more sensitive the PI, the greater the security safeguards required to protect it. It is up to an organisation to determine what is appropriate in the particular circumstances. The Office of the Privacy Commissioner of Canada, which oversees PIPEDA, has released guidance that states that while some information (health and

financial, etc) is always considered sensitive and subject to more stringent protections, any PI could be considered sensitive depending on the context.

In addition, the vast majority of provinces have health legislation that applies specifically to entities that fit within the definition of ‘custodians’ or ‘trustees’ and have stricter and more specific standards of security safeguards for health PI.

Data handling responsibilities of owners of PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Under Canadian private sector privacy law, meaningful consent (either express or implied) is necessary for an organisation’s collection, use and disclosure of PI except in limited circumstances. For consent to be meaningful, individuals must understand the nature, purpose and consequences of what they are consenting to. Under Canada’s federal Personal Information Protection and Electronic Documents Act (PIPEDA), organisations must inform individuals of their privacy management practices, with a particular emphasis on what PI is being collected, with which other organisations their PI might be shared, the purpose for the collection, use or disclosure, and the risk of harm and other consequences that might result from that collection, use or disclosure. Where an organisation is transferring PI to foreign jurisdictions for processing, it must notify the individual that such PI is subject to the laws of that country and may be lawfully accessed there.

In addition, organisations have a general obligation to be open about their policies and practices relating to the management of PI under PIPEDA. Organisations must make certain information readily available to the public in a way that is generally understandable. This includes the contact information of the individual accountable for the organisation’s privacy practices, a description of the type of PI the organisation holds, how an individual can gain access to their PI, a general account of how the organisation uses the PI, what PI is shared with related organisations and a copy of information explaining the organisation's practices. This information typically shows up in website privacy policies, which can only be relied on for consent in certain circumstances (ie, where implied consent is appropriate) because they are often not available until after the collection or use has occurred.

Under PIPEDA, individuals are entitled to be informed of the existence, use and disclosure of their personal information by an organisation, and to access that information, upon making a request in writing. Where an organisation suffers a breach of their security safeguards that creates a real risk of significant harm to the impacted individuals, they must provide notice to the Office of the Privacy Commissioner of Canada (OPC) and those impacted individuals. The notification must be conspicuous and include enough information to allow the individual to

understand the significance of the breach to them and to take steps, if possible, to reduce or mitigate the risk of harm.

Exemptions from transparency obligations
When is notice not required?

Generally, Canadian private sector privacy law is based on consent, which necessarily requires that individuals be provided particular information on which to base their decision to provide or withhold consent to the collection, use or disclosure of their PI. PIPEDA outlines specific exceptions wherein collection, use or disclosure is allowed without the knowledge or consent of the individual. For example, where PI was produced by the individual in the course of their employment and the collection, use or disclosure is consistent with the purposes for which the information was produced. PI can also be collected without knowledge and consent where it would compromise the availability or accuracy of the information and the collection is reasonable for purposes related to investigation a breach of contract or law. These are only a few examples.

Control of use
Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Generally, individuals have the right to acquire information as to an organisation's PII handling practices and policies without unreasonable effort. Individuals also have the right:

- to gain access to their PII;
- to know whether and what type of PII is held;
- a general account of the use and disclosure of their PII; and
- the right to amend PII if it is inaccurate or incomplete.

Data accuracy
Does the law impose standards in relation to the quality, currency and accuracy of PI?

Canadian privacy legislation contains obligations for organisations to ensure that the PI that it uses, collects and discloses is accurate, complete and up to date, particularly where the information is used to make a decision about the individual to whom the information relates or is likely to be disclosed to another organisation.

Data minimisation
Does the law restrict the types or volume of PI that may be collected?

Canadian private sector privacy legislation provides that the amount of PI that an organisation collects should be limited to what is necessary for the identified purpose. Organisations cannot require individuals to consent to the collection, use or disclosure of PI

as a condition for providing a product or service beyond that required to fulfil the explicitly specified and legitimate purpose.

Purpose limitation
Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Under PIPEDA, the purpose for which PI is collected must be one that a reasonable person would consider appropriate in the circumstances. Organisations are generally required to identify the purposes for which PI is collected at or before the time of collection. PI must not be used or disclosed for a new or other purpose, except with fresh consent of the individual or as permitted or required by law.

If an organisation wishes to use PI in its possession for a new purpose, it must obtain fresh consent from individuals to use their PI for the newly identified purpose.

Use for new purposes
If there are purpose limitations built into the law, how do they apply?

If an organisation wishes to use personal information (PI) in its possession for a new purpose, it must obtain fresh consent from individuals to use their PI for the newly identified purpose.

Law stated date

Correct on
Give the date on which the information above is accurate.

24 May 2022.

While care is taken to ensure the accuracy for the purposes stated, before relying upon these articles, you should seek and be guided by legal advice based on your specific circumstances. We would be pleased to provide you with our assistance on any of the issues raised in these articles.

