Online Consent

Frequently Asked Questions

Office of the Privacy Commissioner of Canada

Q. Is consent required for information that is accessible to the public?

A. In the online environment, the distinction between public and private is often blurred. We often upload our information for the purpose of sharing it with an audience, which can be as small as our family or as large as the whole Internet. Organizations might be tempted to collect personal information that they consider as being public, because it is widely accessible, without obtaining consent.

Under PIPEDA, knowledge and consent for certain purposes are not required when information meets the definition of "publicly available." However, "publicly available information" should not be confused with "information that is accessible to the public." In fact, the definition of "publicly available" under PIPEDA is very restrictive.

PIPEDA Regulations define "publicly available" information as information appearing in telephone directories, professional or business directories, government registry information, and records of quasi-judicial bodies that are available to the public. Generally speaking, no consent is required as long as the collection, use and disclosure of such information **relates directly to the purposes for which it was made publicly available.**

"Publicly available" information also includes information published in a magazine, book or newspaper that is available to the public and where the individual has provided the information.

All personal information that is not "publicly available" as defined above, or which is not covered by the other exceptions, requires consent.

For further information, please refer to our Interpretation Bulletin on publicly available personal information.

Q. When is consent valid?

The consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

Q. When is consent not required?

A. PIPEDA contains a list of exceptions for which consent is not required for collection, use, and /or disclosure. The main exceptions to consent are:

- if the collection and use are clearly in the interests of the individual and consent cannot be obtained in a timely manner;
- if the collection and use with consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
- if disclosure is required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records;
- if the disclosure is made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;
- if the disclosure is made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud
- if required by law.

For a complete list of exceptions, please consult section 7, 7.2 and 7.3 of PIPEDA.

Q. Who is responsible for consent when processing of information is outsourced to third parties?

A. Organizations are accountable for protecting personal information that is transferred under outsourcing arrangements. A transfer is considered to be a use of personal information by the organization, such as transferring customer data to a cloud provider for the purpose of storing data. The transferring organization is accountable for the information in the hands of the organization to which it has been transferred.

Organizations should be transparent about transferring information to third parties, especially if they are located in foreign jurisdictions. Organizations should be clear in explaining what information is shared with third parties and what the third party will do with that information. The explanation should be available at or before the time of collection. Organizations must be transparent about their personal information handling practices. This includes advising customers that their personal information may be sent to another jurisdiction for processing and that while the information is in another jurisdiction it may be accessible to courts, law enforcement and national security authorities in that jurisdiction.

With regard to consent, if the third party is using the information for the purpose it was originally collected, additional consent for the transfer is not required. Once individuals have consented to do business with a particular company, they cannot refuse to have their information transferred to a third party for processing, as long as the purpose stays the same.[1] However, they do need to be notified accordingly.

Q. When should an online Privacy Policy be updated?

A. Organizations should review their privacy policies on a regular basis to ensure that they continue to accurately reflect their personal information handling practices. Privacy policies should be updated as necessary. As a best practice, privacy policies should include the date on which the policy became effective. This will give an indication to users whether the organization is making an effort to keep the privacy policy current.

The privacy policy serves as a mechanism for obtaining users' consent to the organization's privacy practices. Whenever an organization plans to introduce significant changes to the privacy policy, it should notify users in advance and consider asking them to confirm their consent prior to the changes coming into effect. Significant changes include a new arrangement to share personal information with a third party, or using personal information for a new purpose.

As a best practice, organizations should periodically audit their information management practices to ensure that personal information is being handled in the way described by their privacy policy.

Q. Are organizations obligated to adopt creative, dynamic and interactive approaches to obtaining consent online?

A. It is up to an organization to decide how to obtain meaningful consent in a way that is best suited to its business. However, binary, static and one-time consent mechanisms are often not effective in a fast-paced online environment. Creative options should be explored in order to ensure that approaches to consent are appropriate to the circumstances and that users are in a position to make meaningful decisions affecting their personal information.

[1] For additional information on cross-border transfers, see "Guidelines for Processing Data Across Borders"