

Prioritizing privacy

5 tips to help you get started

COMPANIES NEED to understand and manage privacy obligations at the outset. Entrepreneurs tend to leave privacy off the list of areas to invest in when starting out. They often use privacy policy templates and generators to quickly put something up on their website and sign up with third-party service providers without thinking about privacy consequences. These practices are risky and it is difficult to play catch-up, especially when consent is required prior to receiving personal information.

To ensure your business complies with Canadian privacy laws, consider the following:

1 Hire a privacy officer and train your employees

An organization is responsible for the personal information under its control. In order to properly protect and handle that information, designate a privacy officer responsible for ensuring compliance. The privacy officer should ensure that there are policies and procedures in place to protect personal information and have a security incident plan ready in case of a breach.

In addition, provide periodic training to staff accessing personal information to apprise them of general privacy obligations and how to handle personal information. This will keep staff well informed and limit privacy breaches due to human error.

2 Create a privacy policy unique to your business

Organizations are required to provide their users with a privacy policy explaining their personal information management policies and practices. Privacy templates or the use of general boilerplate language can leave organizations vulnerable, as they often do not match their specific practices.

In order to avoid this, draft a privacy policy

in plain language that identifies the purpose for which personal information is collected and the specific information collected to fulfill that purpose. Make sure your organization does not collect more information than necessary to fulfill its stated purpose and retains the personal information for only as long as necessary. If your organization discloses personal information to third parties or allows information to cross borders, include provisions disclosing this in your privacy policy. It is also important to inform users they can opt out of providing personal information, if applicable, and how to contact the organization should they have questions or complaints. Update your privacy policy regularly and ensure that it is accessible. Lastly, implement protocols to ensure compliance with the privacy policy.

3 Obtain valid and meaningful consent

An essential aspect of Canadian privacy laws is obtaining meaningful consent prior to collecting, using, and/or disclosing personal information. This includes consent prior to sharing user information with third parties. Meaningful consent requires that users understand what they are consenting to. Moreover, a user's consent applies only to the specific purposes for which their information was initially collected. Fresh consent is required if the purpose for the use or disclosure of personal information changes.

Periodic reminders to users regarding the consent choices they have made and those available to them, as well as context and time-specific consent requests are ways to ensure your organization continues to obtain meaningful consent.

4 Use appropriate safeguards to protect personal information

Organizations are required to protect users'

Brought to you by


**Bereskin
& Parr**

personal information against loss, theft, unauthorized access, disclosure, use, copying, or modification. Protection should be proportional to the sensitivity of the information collected. Consider the necessary physical measures (e.g., alarm systems), technological tools (e.g., password encryption, firewalls), and organizational controls (e.g., limiting access, staff training) that can best protect the information. When determining what kind of safeguards to use, it is worthwhile to consider:

- the sensitivity of the information and the risk of harm to the individuals if that information was breached,
- the format of the information,
- the type of storage used, and
- the types and levels of potential risk your organization faces.

5 Use contractual provisions to manage third-party use of personal information

An organization is responsible for personal information that it entrusts to a third party, for example, for processing. Ensure that contracts with third parties have provisions related to both confidential information and privacy information. These provisions should include requirements for training and auditing, ensure purpose-driven use only, address retention, and ensure that the third party will safeguard the personal information with the level of protection required under Canadian privacy laws.

While these 5 tips are helpful in getting started, reach out to a privacy professional for advice customized to your privacy needs. 

Melanie Szwera is a partner with Bereskin & Parr LLP and co-leader of the Privacy/Regulatory, Advertising, and Marketing practice group. Her expertise includes patent prosecution and Canadian privacy matters.



Parnian Soltanipناه is an associate with Bereskin & Parr LLP in the Life Science and Privacy Law practice groups. She assists in patent prosecution and advises on compliance with Canadian privacy laws.

