Office of the Information & Privacy Commissioner
for British Columbia
Protecting privacy. Promoting transparency.

PRIVACYRIGHT
fundamentals for business

How to write a privacy policy

Today’s webinar covers how to write a privacy policy for your organization.

So what exactly is a privacy policy? Well, a privacy policy explains how and why your organization handles PI. It helps others understand *why* your organization collects PI, *how* the PI will be protected, and who to contact if you have questions or concerns. You can also use your privacy policy to train your staff.

Your privacy policy is a very important part of your privacy management program. Use plain language when writing your policy, so the content is easy for everyone to understand. PIPA requires privacy policies be available upon request – posting your privacy policy on your website is an easy way to accomplish this!

The first few elements you should include are pretty easy to document, especially if you’ve already given some thought to your personal information inventory. For example, privacy policies should start with a description of the types of PI collected, who the PI is about, and how it will be used by folks within your organization.

Next, it is important to document whether your organization will notify individuals and seek consent before collecting PI. If so, how will you do this? Note that under PIPA, individuals have the right to withdraw consent at any time.

You must inform individuals how and when their PI may be disclosed to others. Some examples may include disclosure to third party service providers, government bodies, or the police.

Your privacy policy should also document how long you intend to retain the PI. PIPA requires that organizations destroy PI once it is no longer necessary for legal or business purposes.

Keep in mind that under PIPA, organizations must retain PI for at least one year if it was used to make a decision that directly affects someone. This gives individuals the opportunity to request access to their own PI.

Your policy should provide information on how your organization will destroy the PI after you no longer need it.

Next, your privacy policy should also provide details about how you intend to protect the PI from unauthorized access or a privacy breach.

There are many security safeguards your organization can put in place to protect the PI you collect – from policies, training, and written procedures for how staff should report suspected breaches – to physical safeguards, like locking up records and having security screens on your computers. There are also technological safeguards to consider, like using unique logins and passwords for each employee and encrypting any PI stored or carried on a mobile device (such as a USB or laptop). We have a separate webinar dedicated to security safeguards, so make sure to check it out on our website.

The final elements in your privacy policy address communication with the people whose PI you have collected or used. Let these individuals know that that they have a right to access their own PI and to request corrections. Be transparent and helpful! Provide instructions on how they can request access or corrections.

Your policy should also contain information about how someone can make a complaint about your organization’s collection, use or disclosure of PI.

Be sure to include contact information for your privacy officer. And finally, don’t forget to let people know that they can contact us at the OIPC as well.