Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

PRIVACYRIGHT fundamentals for business

Understanding notification and consent

Today's webinar covers why notification and consent matter under PIPA.

Consent is a very important part of PIPA. With very few exceptions, organizations *must* get consent before collecting, using, or disclosing personal information about an individual.

There are three types of consent under PIPA ….

- There is express consent, which can be verbal or written. Express consent is when a business provides notification so that the person is fully aware of how and why their PI is being collected. The individual then willingly agrees to this action.

- **Implied consent** can also be written or verbal. However, notification is not needed because the purpose for collecting this personal information is obvious, and does not need any further explanation for the individual to be fully informed.

- "**Opt-out consent,**" the third type of consent, requires your organization to notify a person of the intended use of their PI, and then give them the option to not participate by un-checking an agreement box.

Your organization must create conditions for the consent first, **before** individuals can consent to the collection, use and disclosure of their personal information. The conditions are ensuring the collection is appropriate and that you have given adequate notification.

Well, first, you must establish that there is an appropriate purpose for the collection, use, or disclosure of the PI.

Use the 'Reasonable Person Test' to evaluate the purpose of the collection, use, and disclosure of PI by your organization.

The reasonable person test considers the nature of the information collected, the purposes and circumstances surrounding the collection and the use of the information, and how the organization handles the information. Think about whether a reasonable person with no special interest would consider your intended collection, use, and disclosure of the personal information to be appropriate.

Second, organizations must provide adequate notification by **notifying** the individual of the purpose for the collection, use, or disclosure of personal information. This means that

organizations must give individuals enough information to allow them make an informed decision about whether or not to give consent.

There is one important exception: implied consent. If the collection of PI is obvious to a reasonable person, then PIPA **doesn't** require written or verbal consent.

Now, we'd like to share a few final tips. First, make sure the notification is transparent. Use plain language, and address these three questions:

1. Is the notification easy to understand?
2. Is the purpose for collecting PI clear?
3. Is it clear how PI will be used or disclosed?

Here's another tip, or rather, cautionary note: If the notification contains false or misleading information, OR if your organization uses deceptive or misleading practices to get consent, the consent is invalid. Further, if your organization uses deception or coercion to collect personal information, this would be an offence under PIPA. The individual or organization responsible can be prosecuted, and the affected individual would also be able to sue for damages.

Remember, individuals can only provide meaningful consent **after** you've established a reasonable **purpose AND** after you have provided **adequate** notification.

Under PIPA an individual also has the right to **withdraw** or change consent.

Organizations cannot ***require*** **consent** unless it is necessary or integral to providing a product or service.

What if you want to change how you handle the PI you've collected or who you want to share it with? Well, in that case, you have to provide individuals with notification and obtain their consent for the new uses or disclosures.

PIPA does not specify a minimum age for consent.
If a minor is capable of understanding what they are consenting to, they may consent, regardless of age. Age 12 is generally recognized as old enough for a minor to consent but this can vary based on the individual and circumstances for collection of the PI.

There are also certain limited situations where PIPA permits the collection, use or disclosure of PI **without consent** from a source other than the individuals who the PI is about. For example, you can collect PI without consent or notification when:

1. it is clearly in the interests of the individual and consent cannot be obtained in a timely way.;
2. the PI is necessary for medical treatment and the individual is unable to give consent;
3. the PI is collected visually at a public performance, sports meet or similar event that the individual voluntarily attends;
4. the information is used to decide if an individual is suitable for an honour, award or other similar benefit;
5. the information is necessary to collect or pay a debt owed to or by the organization; or
6. it is required by law.

Ok, let's discuss employee personal information. PIPA treats employee PI a bit differently than other personal PI.
Here's why: Employee PI is PI about the **individual** that is collected, used or disclosed *solely* for purposes required to establish, manage or terminate an employment relationship.
For the purposes of PIPA, this applies to current and prospective employees, volunteers, and candidates.

PIPA allows organizations to collect employee PI without consent if the same circumstances we just discussed for collecting other PI without consent apply. Organizations can also collect personal information for managing or terminating employment. But you still have to **notify** the employee that you are collecting or using their PI, and give them the reason why.

Here are a couple of examples. Let's say you post a job and an applicant sends you their resume. Or maybe you want to promote someone from within your organization. In both these cases, consent is implied, because the PI is relevant to the hiring decision.

Consent is implied for checking an interviewee's relevant qualification, , past job experience, knowledge, skills and abilities," and answers to interview questions and skills tests.

What about just searching Facebook for information about a potential employee? Well, this is a bit of a gray area. Here's why: When you check out someone on Facebook you risk collecting inaccurate or irrelevant information, too much information, and the PI of others.
That's why organizations cannot rely on consent for social media background checks. You should only perform a social media background check if you can demonstrate you have the proper legal authority.

Remember, as we mentioned earlier, any collection of PI, must be limited to what a reasonable person would consider appropriate in the circumstances.
What does this mean when it comes to employee PI?
Well, you have to be able to show that your collection or use of PI is reasonably required in order to determine the job applicant's suitability for the position.

OK! Now that we've established that your collection of PI is reasonable, let's move on to how you can obtain consent online.

Most organizations have a webpage where they advertise their services or products. Or maybe there is an option to submit questions or request a quote for service online. Some organizations even have a login portal for online ordering of products.

In these circumstances, the PI is a little less obvious but can reveal just as much about a person as an address or phone number. Online data can include:

- Location information, including GPS data;
- Unique device identifiers, such as IP and MAC or media access control address;
- Click stream data, browser history, bookmarks; and
- User generated social network data such as comments, ratings, likes and dislikes, twitter stream, and customer service transactions.

The bottom line? No matter how your website it set up, if you are collecting PI from visitors to your website or your social media page, you need to provide adequate notification of how their personal information will be collected, used, or disclosed.

What's the best way to accomplish this? Well, make sure you have a clear, detailed, and easily accessible privacy policy on your website.

Make sure your policy is easy for your visitors to find. You should also include contact information for your privacy officer for anyone who has questions or concerns.

Now that I've shared the basic requirements for providing meaningful notification and obtaining informed consent, here are some final reminders to think about, whether you are collecting PI in person, online, or from third parties:

1. Only collect, use or disclose PI for purposes that a reasonable person would consider appropriate, under the circumstances.
2. Notifications should clearly explain what information you collect, how you use it, and who you share it with.
3. You must inform individuals and obtain consent again if you make significant changes to how you handle the PI, for instance, if you want to use it for new purposes or disclose the PI to new third parties.
4. Allow individuals to withdraw consent, if they are not otherwise bound by legal or contractual restrictions.

5. Provide contact information for your privacy officer in case anyone has questions about the collection, use or disclosure of their PI, your privacy policy, or about how your organization will safeguard the PI you collects.
6. Finally, obtaining consent does not release organizations from obligations under privacy laws. Remember - you are accountable for safeguarding the information your organization collects, uses and discloses.