BRITISH COLUMBIA PRIVACY COMMISSIONER RELEASES GUIDANCE ON COLLECTING PERSONAL INFORMATION FOR POLITICAL ACTIVITIES

Posted on November 1, 2022

Categories: Insights, Publications

On August 30, 2022, the Office of the Privacy Commissioner of British Columbia ("**OIPC**") released guidance on best practices to follow for political organizations handling personal information as part of the political campaigning process (the "**Guidance**").[1] The Guidance was released shortly after the OIPC released a decision on March 1, 2022, stating that BC's *Personal Information Protection Act* ("**PIPA**")[2] applies to federal political parties as well as provincial political parties.[3] The Guidance is intended to ensure that political organizations, whether federal or provincial, conform to PIPA when campaigning.

Obtaining Proper Consent

As with all private organizations, the first step in handling personal information is obtaining meaningful consent. However, securing consent may not be required when personal information is taken from public sources of information, including telephone or professional directories, government registries, and certain electronic publications such as newspapers. Consent may also not be required where collection is otherwise authorized by law, such as through the *Election Act*.

When consent is required, organizations must ensure that the consent which they secure is meaningful. In addition, PIPA also requires an organization to provide a notification statement when obtaining consent. The purpose of the notification statement is to inform individuals before or at the time of collection as to the purpose of the collection, and to provide the contact information of someone in the organization to whom an individual can go with any questions. To that end, the Guidance sets out a series of best practices which organizations can follow to help them ensure that they obtain meaningful consent and draft compliant notification statements. The Guidance even provides a sample notification statement for political organizations to follow.[4]

OIPC has provided similar guidelines for private organizations, to ensure that they understand the requirements around obtaining clear, informed and meaningful consent.

Reasonable Purposes

Even when an organization concludes that consent is required and they have obtained that consent in a meaningful fashion, those are only the first steps which the organization must take. The Guidance explicitly provides that, regardless of consent, organizations can only collect, use, and disclose personal information for reasonable purposes. The OIPC then proceeds to give examples of both when purposes are likely to be reasonable in the context of a political campaign as well as, and arguably more importantly, when purposes are NOT reasonable. Some of the examples of unreasonable purposes include:

- any purpose requiring collection, use or disclosure of biometric information;
- using an automated system to communicate with and collect voter information where the voter may be unaware they are communicating with a robot;
- trying to guess age, gender or ethnicity from already collected information;
- collecting and using personal information from social media beyond what is needed to respond to individuals; and
- using facial recognition technology.

Again, the position of the OIPC in the Guidance follows trends in guidance from other privacy commissioners across Canada who are stressing the sensitivity of biometric information, restrictions on using social media, and the risks of using artificial intelligence or automated systems when collective, using or processing personal information.

Keeping Information Secure

Once collected, personal information must be kept secure. Organizations must make reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal of personal information through a robust privacy management program.[5] The Guidance provides best practices for creating and maintaining a strong privacy management program, including:

- implementing an open and transparent privacy policy;
- providing reasonable security for personal information, including use of personal devices;
- conducting risk assessments on the organization's activities;
- retaining information only as long as needed and securely destroying information no longer needed or out-of-date;
- only providing access to personal information to individuals who require it; and
- ensuring third party contracts follow the organization's standards for security and handling of personal information.

PIPA requires that individuals have the ability to access their own personal information.[6] The Guidance recommends that if requested, political organizations should provide all of the requestor's personal information under or within their control, inform the requestor about the ways they have used or are using that person's personal information, and inform the requestor to whom their personal information has been disclosed.

Application to service providers

Political organizations, just like other organizations, often use third party contractors or service providers to perform certain work. However, engaging such third party contractors or service providers does not absolve the political organization of its responsibilities under PIPA. Rather, the political organization remains responsible for the protection and appropriate use of the personal information, even if a service provider may have custody of that personal information. The Guidance provides the following important considerations to consider when engaging service providers:

- be attentive to broad licencing terms in software that may allow a service provided unlimited access to data and the power to sell or distribute that data to additional third parties, particularly if a service provider advertises "free" services;
- consider what type of personal information is being handed over, as some information is particularly sensitive and requires extra care (such as biometric information); and
- avoid service providers with poor track records on data security (do your due diligence on any third party before engaging them).

Conclusion

The Guidance is important for political organizations, as well as any service providers or third party contractors who work with them. It stresses the level of diligence required when collecting, using, storing, and disclosing personal information as part of both provincial and federal elections and other political activities.

Whether you require help drafting notification statements, understanding when and how to obtain meaningful consent, or if your particular situation constitutes a reasonable purpose that permits the collection of information, our Privacy and Data Protection Group can provide advice to ensure that all PIPA requirements are met.

[1] The Office of the Privacy Commissioner of British Columbia, *Political Campaign Activity* (August 30, 2022), available here.
[2] *Personal Information Protection Act*, SBC 2003, c, C-63 ("PIPA").
[3] *Conservative Party of Canada (Re)*, 2022 BCIPC 13.

[4] See page 3 of the Guidance.
[5] PIPA, s 34.
[6] PIPA, s 23.

by Robert Piasentin, Kristen Shaw and Navaneeth Ravichandran (Articled Student)

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.