Guidance for federal political parties on protecting personal information

Overview

Political parties may collect, use and disclose highly sensitive personal information in the course of their activities. No federal privacy laws currently apply to federal political parties. At this time, British Columbia is the only jurisdiction in Canada that regulates the privacy practices of political parties.

In December 2018, Parliament enacted Bill C-76, the *Elections Modernization Act*. Bill C-76 amended the *Canada Elections Act* (CEA) to require political parties to develop specific privacy policies, to submit those policies to Elections Canada and to publish them online.

The Office of the Privacy Commissioner of Canada (OPC)and the Chief Electoral Officer (CEO) have prepared this guidance to assist federal political parties in complying with their new legal obligations relating to privacy policies. While these policies must have prescribed content, they do not require the substance to comply with international privacy standards. However, we encourage political parties to take this step.

This guidance also outlines a number of best privacy practices based on international law standards - which political parties are encouraged to follow - in order to protect the personal information in their care better and help engender trust among Canadians.

This page is for

Federal political parties and all those associated with such parties and federal election campaigns, including candidates, incumbents, staff and volunteers.

Who to contact

The OPC has no oversight role with respect to the obligations imposed by Bill C-76. The OPC is therefore not in a position to receive or investigate complaints with respect to matters covered in this guidance that do not otherwise fall within its jurisdiction under the *Personal Information Protection and Electronic Documents Act* or the *Privacy Act*.

Individuals with specific concerns should first contact the listed privacy officer of the political party in question (as outlined in their policy) and/or Elections Canada if they have concerns about the accuracy of a party's policies. The CEO may consult the OPC as required.

On this page

- Legal obligations
- Privacy best practices
- Key concepts in data protection, useful links, examples and resources

Legal obligations for privacy policies

With the new legal requirements in force, federal political parties are required to publish a privacy policy on their website and submit it to Elections Canada as a condition of registration.[1] If the privacy policy is changed, the party must inform the CEO and update the online version of its policy. The privacy policy will have to contain the following elements[2] (left column) while the illustrative examples provided (right column) are drawn from recent reports on the privacy practices of political parties in British Columbia, Quebec and the United Kingdom.

Required Elements	Examples
(i) a statement indicating the types of personal information that the party collects and how it collects that information.	Does the party collect personal information relating to an elector's income, residence, family members, ethnicity, political views or affiliation, etc.? Does the party collect information on party members such as contact information? Does the party collect electors' financial information? Is personal information purchased from a data broker, collected via social media, gathered via petitions, or any other means?
(ii) a statement indicating how the party protects personal information under its control.	How is personal information protected? By encrypting electronic data, keeping paper information in locked filing cabinets, limiting who in the party has access to it, ensuring network protections and firewalls are up to date, etc.?
(iii) a statement indicating how the party uses personal information under its control and under what circumstances that personal information may be sold to any person or entity.	Will membership lists be used for political activities such as fundraising, volunteer drives and canvassing? Are voter profiles developed and how are they used? Will voter profiles and party databases be shared with provincial parties, or sold to any groups or individuals?
(iv) a statement indicating the training concerning the collection and use of personal information to be given to any employee of the party who could have access to personal information under the party's control.	How will party officials be trained in safeguarding personal information and acceptable disclosure practices? How will volunteers be trained in collection of information during canvassing and ensuring it is protected against loss or theft?
(v) a statement indicating the party's practices concerning: (A) the collection and use of personal information created from online activity, and, (B) its use of cookies.	Will personal information be collected through the use of cookie files, social media monitoring, dedicated mobile applications, public / private settings, etc.?

[1] *Canada Elections Act*, S.C. 2000, c. 9, ss. 385(2)(k),385(4), 385.1
[2] *Canada Elections Act*, S.C. 2000, c. 9, s. 385(2)(k)

(vi) the name and contact information of a person to whom concerns regarding the party's policy for the protection of personal information can be addressed.	The specific name and contact information for a party employee who can address public concerns around privacy.

Best practices based on international law standards

Individuals expect political parties to respect their privacy. A good privacy policy is one of the important ways in which an organization can accomplish this. While the new law prescribes some elements of content, it does not require that content comply with international privacy standards. Adhering to fair information principles will give meaning to those policies and help parties ensure personal information is treated in a manner respecting the privacy rights of Canadians.

Fair Information Principles	Best Practices
Principle 1 - Accountability	Political parties should: • Implement policies and procedures to protect all personal information in accordance with the ten privacy principles outlined in this table. • Put in place contracts detailing how personal information will be protected when hiring third parties such as service providers. • Be ready to demonstrate that they are treating personal information with an appropriate level of care. For example, keep policies in writing and maintain records that can be reviewed to establish compliance. • Inform affected individuals of any breach of personal information that poses a significant risk of harm.
Principle 2 - Identifying Purposes	Political parties should: • Document and be transparent about why personal information is collected, what it will be used for, and why it may be shared with other organizations. • Identify any new purpose for the information and obtain the individual's consent before using it. • If, for example, a political party wishes to use petition information for any purpose other than the purpose of promoting the issue raised in the petition, this should be specified.
Principle 3 - Consent	Political parties should: • Obtain consent to collect, use or disclose personal information[3], including: ○ Inferred data (this includes use of observational data to estimate age, gender or financial status)

[3] An exception to the consent principle in the context of political parties is the National Register of Electors. Elections Canada compiles this information from a variety of other federal and provincial agencies. Elections Canada, as a legal requirement of the *Canada Elections Act*, distributes lists of electors to parties and candidates.

Fair Information Principles	Best Practices
Principle 3 - Consent	○ Predictive data (this may include using sensitive data such as political opinions, ethnicity or religious affiliation to forecast voting choices) • Obtain valid consent from individuals by ensuring they are informed of the following when asking for their personal information: ○ What is being collected ○ What it will be used for ○ To whom it will be disclosed ○ Any consequences they might face as a result of allowing the party to collect and use their personal information • Only use personal information for purposes individuals have consented to. For example, do not collect personal information on political views, religion or ethnicity without express consent. • Similarly, do not assume consent to add personal information collected through social media to party databases simply when individuals interact with a party by liking a post or an article on social media. • Refrain from collecting information from individuals that pertain to others, such as family members or neighbours. • Verify that consent was obtained when receiving personal information from third parties, such as data brokers. • Seek consent before disclosing personal information (for instance, before uploading political party internal contact lists to social media platforms).
Principle 4 - Limiting Collection	Political parties should: • Avoid indiscriminate collection by limiting the amount and types of personal information gathered to what is necessary for the identified purposes. • For example, canvassers should not record opinions of a respondent about the assumed attitudes and voting intentions of others in the same household. • Do not deceive or mislead individuals about why their personal information is collected.
Principle 5 - Limiting Use, Disclosure, and Retention	Political parties should: • Only use or disclose personal information for purposes relating to the original purpose of the collection. • For example, information collected for a specific petition or cause should not be reused for general political messaging. • For example, do not disclose email addresses or other identifiers to social media platforms for data analysis or profiling without express consent. • Keep personal information only as long as necessary to satisfy those purposes, and then destroy the information securely. • Have procedures for retaining and destroying personal information.
Principle 6 – Accuracy	Political parties should: • Ensure that the personal information they hold is accurate and up to date. This will minimize the possibility of using incorrect information when making a decision about an individual, or when disclosing information to third parties.

Fair Information Principles	Best Practices
	• Parties should bear this in mind when drawing inferences, for example, about voters or relying on those supplied by third parties. • To the greatest extent possible, political parties should ensure that their inferences are accurate.
Principle 7 - Safeguards	Political parties should: • Protect information from unauthorized access, disclosure, copying, use or modification, regardless of format (i.e. electronic or paper). • Use a combination of security safeguards based on the sensitivity of the information held. • For example, political opinions, health status, religious background, ethnicity and financial information can be considered very sensitive and should be subject to stricter safeguards. • Safeguards can include encryption, locked cabinets and limiting access to those who need to know it. • Parties should make their employees, volunteers and contractors aware of the importance of maintaining the confidentiality of personal information.
Principle 8 - Openness	Political parties should: • Be transparent, clear and accountable about their personal information management practices. • For example, if voters are sorted based on political opinions, party allegiance, personal interests, language, ethnic origin or education, this should be made clear. • Ensure privacy communications are easy to understand regardless of the device they may be read on, and that they are made available in a variety of ways (e.g. in person, in writing, by telephone, in publications and on your organization's website).
Principle 9 - Individual Access	Political parties should: • Give individuals access to their information upon request, including any inferences or predictions made about them. • Be able to provide an account of how information has been used and of all disclosures of personal information to third parties, if requested. • Correct or amend any personal information if its accuracy or completeness is challenged and found to be outdated. • For example, upon request, parties should provide all personal information on an individual the organization retains, describe how that information has been and is being used, and detail if that information has been disclosed.
Principle 10 - Challenging Compliance	Political parties should: • Provide recourse by developing simple complaint handling and investigation procedures.

Fair Information Principles	Best Practices
	• Advise people raising concerns about their avenues of recourse. • Ensure all complaints are investigated.

Key concepts in data protection, useful links, examples and resources

Links to OPC quick tips

- 10 Privacy tips for business infographic
- 10 Tips for a Better Online Privacy Policy and Improved Privacy Practice Transparency

Links to detailed OPC guidance

- Privacy Toolkit for Businesses
- PIPEDA fair information principles
- Guidelines for obtaining meaningful consent

Links to provincial guidance for political parties

- BC OIPC Report: Full Disclosure: Political parties, campaign data, and voter consent
- Élections Québec report: Partis politiques et protection des renseignements personnels (only available in French)

Links to international guidance for political parties

- European Commission "Protecting Europeans' personal data in elections"
- UK ICO "Guidance on political campaigning" and "Investigation into the use of data analytics in political campaigns"
- CNIL « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ? » (only available in French)
- CNIL "Élections législatives : six réflexes pour une campagne 2.0 responsable » (only available in French)

Links to academic reviews of Canadian parties and privacy

- Bennett, Colin, "Data Driven Elections and Political Parties in Canada: Privacy Implications, Privacy Policies and Privacy Obligations" (April 2018). *Canadian Journal of Law and Information Technology;*
- Elizabeth Judge and Michael Pal, "Privacy and the Electorate: Big Data and the Personalization of Politics" (October 2014).